aws

ユーザーガイド

AWS Elemental MediaConnect

AWS Elemental MediaConnect: ユーザーガイド

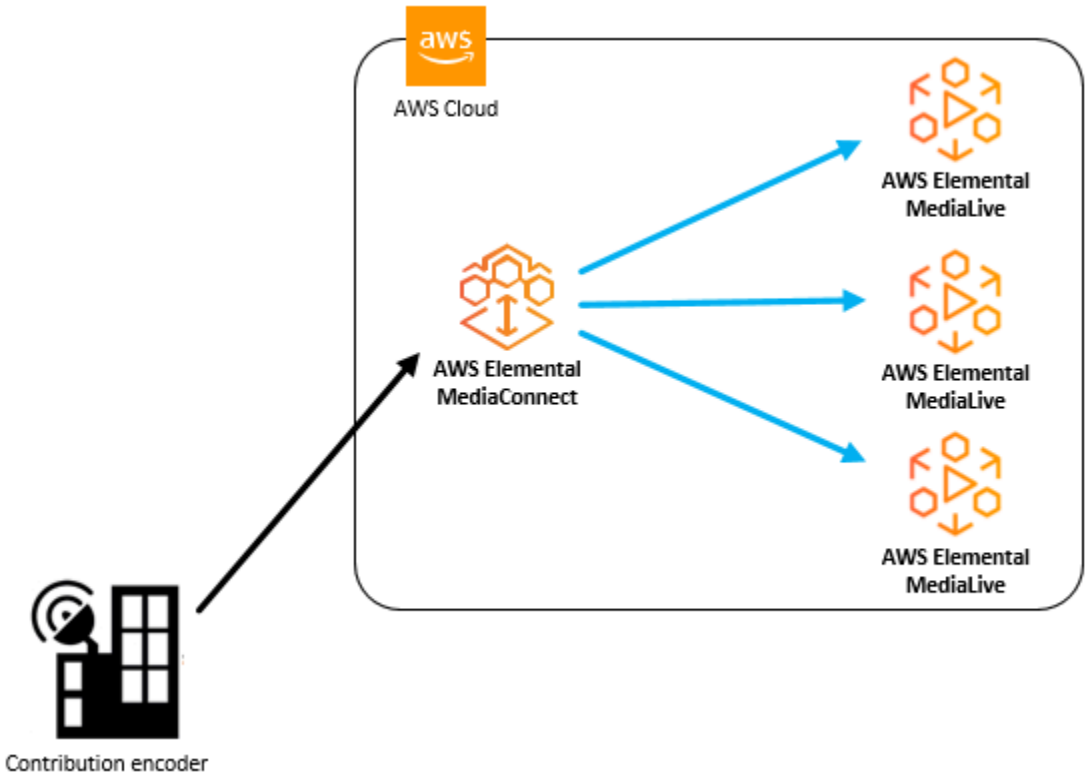
Table of Contents

AWS Elemental MediaConnect とは?

AWS Elemental MediaConnect は、ブロードキャスターとその他のプレミアムビデオプロバイダーが、信頼性に優れた方法でライブビデオを AWS クラウドに取り込み、それを AWS クラウド内外の複数の宛先に配信できるサービスです。MediaConnect では、既存のディストリビューション方法で慣れ親しんでいる信頼性、セキュリティ、可視性が得られるのに加えて、インターネットベースの送信が提供する柔軟性と費用対効果も得られます。

取り込みでは、オンプレミスのコントリビューションエンコーダーから AWS Elemental MediaConnect にコンテンツを送信します。これにより、動画が単一の高品質メザニンファイルにエンコードされ、クラウドにコントリビューションされます。動画が AWS クラウドに保存されると、MediaConnect はクラウドエンコーダー、別の MediaConnect フロー、オンプレミスの送信先など、指定された出力に動画を送信します。

次の図は、AWS Elemental MediaConnect がライブ動画をクラウドに取り込み、複数の宛先にセキュアに配信する方法について基本的なワークフローを示しています。



AWS Elemental MediaConnect では、ソースと 1 つ以上の出力間のトランスポートを確立するフローを作成します。エンタイトルメントを作成することで、他の AWS アカウントとコンテンツを共

有することもできます。これにより、受信アカウントはコンテンツをソースとして使用してフローを作成できます。

AWS Elemental MediaConnect では、次のことを実行できます。

- ライブ動画を AWS クラウドに取り込みます。
- ライブ動画を AWS クラウド内外の複数の宛先に配信します。
- 別の AWS アカウントから提供されたライブ動画ストリームをサブスクライブします。(これには、エンタイトルメントを通じてコンテンツ制作者からの許可が必要です)。
- ある AWS リージョンから別のリージョンにコンテンツを送信します。

トピック

MediaConnect の概念と用語

ARN

すべての AWS リソースに固有の識別子である [Amazon リソースネーム] です。

アベイラビリティーゾーン

AWS クラウドコンピューティングリソースがホストされている特定の場所。AWS リージョン内のアベイラビリティーゾーンは、低レイテンシー、高スループット、そして高冗長性のネットワークにより接続されています。さらに、それらは物理的に分割され、互いに分離されています。冗長性を確保するために、異なるアベイラビリティーゾーンに MediaConnect フローを作成するように選択できます。

AWS リージョン

1 つ以上のアベイラビリティーゾーンが配置されている地域。各 AWS リージョンは独立していて、他のリージョンから分離されています。さまざまなリージョンで MediaConnect フローを作成して、世界各地に設置されたレシーバーにコンテンツを配信できます。AWS リージョンとア

ベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

CDI フロー

JPEG XS を使用して軽く圧縮された高品質のコンテンツを転送する MediaConnect フローです。コンテンツは、オーディオ、動画、または補助データ用に別々のメディアストリームに逆多重化されます。各 CDI フローでは、ソースに複数のメディアストリームを使用し、出力ごとに複数のメディアストリームを使用できます。MediaConnect は AWS Cloud Digital Interface (AWS CDI) ネットワーク技術を使用して、SMPTE 2110、パート 22 トランスポート規格に準拠したコンテンツを取り込みます。

コントリビューションエンコーダー

ライブ動画フィードを受信し、ストリームを単一の高品質メザニンストリームにエンコードして転送したり、アダプティブビットレート (ABR) ストリームにさらに処理したりするエンコーダー。

ディストリビューション

コンテンツをさまざまな地域に配信する目的で、他の AWS リージョンの MediaConnect フローに向けた出力を作成した結果です。

エンタイトルメント

AWS アカウントが特定の MediaConnect フロー内にあるコンテンツにアクセスするために付与されるアクセス許可。コンテンツ発信者は、特定の AWS アカウント (サブスクライバー) にエンタイトルメントを付与します。エンタイトルメントが付与されると、サブスクライバーは発信者のフローをソースとして使用してフローを作成できます。エンタイトルメントを付与できるのはトランスポートストリームフローに限られます。

フロー

1 つ以上のビデオソースと 1 つ以上の出力間の接続を作成します。フローごとに、使用するトランスポートプロトコル、暗号化情報、および必要な出力またはエンタイトルメントの詳細を指定します。MediaConnect は、ライブ動画を 1 つのユニキャストストリームとして送信できる取り込みエンドポイントを返します。サービスでは、AWS クラウドの内部または外部を問わず、指定したすべての出力に動画をレプリケートして配信します。フローには、トランスポートストリームと JPEG XS の 2 つのタイプがあります。

メディアストリーム

動画、オーディオ、または補助データを含む単一トラックまたはメディアストリームです。CDI プロトコルまたは ST 2110 JPEG XS プロトコルを使用している限り、メディアストリームをフ

ローに追加すると、そのメディアストリームをそのフロー上のソースと出力に関連付けることができます。各ソースまたは出力は、1 つまたは複数のメディアストリームで構成できます。

メザニンストリーム

低圧縮のビデオストリームで、フル解像度の非圧縮ストリームよりも容量が少なくて済みます。メザニンストリームの品質は、消費者向けデバイスに配信される最終的なエンコードを作成するためのソースとして使用できるほど高画質です。

提供タイプ

毎月特定量のアウトバウンド帯域幅を使用する契約に対して MediaConnect が提供する割引です。サービスを購入する際は、予約を行います。

発信者アカウント

少なくとも 1 つのエンタイトルメントを持つフローの作成に使用された AWS アカウントです。

出力

取り込んだ動画を MediaConnect に送信する宛先です。出力には、ソースと同じプロトコルと異なるプロトコルが含まれます。

ポリシー

AWS でのアクセスを管理するために使用される IAM ポリシーです。

プロトコル

ファイル送信に使用される一連のルールです。MediaConnect には、サービス品質 (QoS) レイヤーを実装するプロトコルオプション (Zixi、RTP、RTP-FEC など) が用意されています。これにより、サービスがメザニン品質のライブ動画と連携できるようになります。

レシーバー

MediaConnect からのストリームの受信側です。レシーバーとは、RTP または Zixi ストリームを受信できる、AWS クラウド内外のあらゆるエンティティです。これは、アフィリエイト、クラウドエンコーダー、または別の MediaConnect フローである可能性があります。

予約する

指定された期間にわたって、毎月特定量のアウトバウンド帯域幅を使用する契約。その代わりに、その帯域幅に対して割引された時間料金を支払います。サービスを購入する際は、予約を行います。

レプリケーション

複数の出力を含むフローを作成した結果です。ソースはレプリケーションされ、複数の出力が生成されます。レプリケーションは、自分のアカウント内の複数のワークフローに動画ストリームを配信したり、コンテンツを他の AWS アカウントと共有したりする場合に便利です。

リソース

操作可能な AWS のエンティティ。各 AWS リソースには、一意の識別子として機能する Amazon リソースネーム (ARN) が割り当てられています。MediaConnect では、リソースとその ARN 形式は次のとおりです。

- エンタイトルメント: `aws:mediaconnect:`*`region`*`:`*`account-id`*`:entitlement:`*`resourceID`*`:`*`resourceName`*
- フロー: `aws:mediaconnect:`*`region`*`:`*`account-id`*`:flow:`*`resourceID`*`:`*`resourceName`*
- 出力: `aws:mediaconnect:`*`region`*`:`*`account-id`*`:output:`*`resourceID`*`:`*`resourceName`*
- ソース: `aws:mediaconnect:`*`region`*`:`*`account-id`*`:source:`*`resourceID`*`:`*`resourceName`*

共有中

別の AWS アカウントがフローのコンテンツにアクセスできるようにします。コンテンツを共有するには、あなた (発信者) が別の AWS アカウント (サブスクライバー) にエンタイトルメントを付与します。

ソース

設定情報 (暗号化とソースタイプ) およびネットワークアドレスを含む外部動画コンテンツです。各フローには少なくとも 1 つのソースがあります。標準ソースは、オンプレミスのエンコーダーなど、別の MediaConnect フロー以外のソースから取得します。使用権限のあるソースは、別の AWS が所有し、アカウントにエンタイトルメントを付与した MediaConnect フローから取得します。

サブスクライバーアカウント

別の AWS アカウント (発信者アカウント) が所有する AWS Elemental MediaConnect フローのコンテンツへのアクセスが許可された AWS アカウント。この許可は、発信者がサブスクライバーの使用権限を設定したときに付与されます。このエンタイトルメントにより、サブスクライバーは送信者のコンテンツをソースとして使用するフローを作成できます。

トランスポートストリームフロー

圧縮されたコンテンツを転送する MediaConnect フローです。オーディオ、動画、および補助データは 1 つのストリームに結合 (多重化する)必要があります。その品質は、消費者向けデバイスに配信される最終的なエンコードを作成するためのソースとして使用できるほど高品質です。出力を追加して、コンテンツの送信先と転送方法を指定できます。エンタイトルメントを付与して、別の AWS アカウントがコンテンツにアクセスできるようにすることもできます。

VPC インターフェイス

フローと Amazon Virtual Private Cloud (Amazon VPC) サービスを使用して作成された、仮想プライベートクラウド (VPC) との接続です。

ホワイトリスト

Classless Inter-Domain Routing (CIDR) IP アドレスのブロックを MediaConnect フローのソースとして使用できるようにします。

関連サービス

- AWS CloudTrail は、AWS マネジメントコンソール、AWS CLI、その他のサービスからの呼び出しを含め、アカウントの CloudTrail API に対する呼び出しをモニタリングできるサービスです。詳細については、「AWS CloudTrailユーザーガイド」を参照してください。
- Amazon CloudWatch は、AWS クラウドリソースと、AWS で実行するアプリケーションのモニタリングサービスです。CloudWatch Events を使用して、AWS Elemental MediaConnect のフローのステータスの変化を追跡します。詳細については、「Amazon CloudWatch のドキュメント」を参照してください。
- AWS Identity and Access Management (IAM) は、AWS リソースへのユーザーアクセスをセキュアに管理するウェブサービスです。IAM を使用して、どのユーザーが AWS リソースを使用できるかを制御し (認証)、さらに、どのリソースをユーザーがどのように使用できるかを制御します (権限付与)。詳細については、「設定」を参照してください。
- AWS Elemental MediaLive は、ブロードキャストおよびストリーミング配信用のライブ出力を簡単かつ確実に作成できる動画サービスです。詳細については、「AWS Elemental MediaLiveユーザーガイド」を参照してください。

MediaConnect へのアクセス

次のいずれかの方法で AWS Elemental MediaConnect にアクセスできます。

- AWS マネジメントコンソール - このガイドの手順では、AWS マネジメントコンソールを使用して MediaConnect のタスクを実行する方法について説明しています。コンソールを使用して MediaConnect にアクセスするには、次のようにします。

```
https://<region>.console.aws.amazon.com/mediaconnect/home
```

- AWS Command Line Interface - 詳細については、「AWS Command Line Interface ユーザーガイド」を参照してください。CLI エンドポイントを使用して MediaConnect にアクセスするには、次のようにします。

```
aws mediaconnect
```

- AWS Elemental MediaConnect API — API アクションの情報と API リクエストの作成方法については、「AWS Elemental MediaConnectAPI リファレンス」を参照してください。REST API エンドポイントを使用して MediaConnect にアクセスするには、次のようにします。

```
https://mediaconnect.<region>.amazonaws.com
```

- AWS SDK – AWS によって SDK が提供されているプログラミング言語を使用している場合は、SDK を使用して AWS Elemental MediaConnect にアクセスできます。SDK では、認証を簡素化し、開発環境と容易に統合して、MediaConnect のコマンドに簡単にアクセスできます。詳細については、「Amazon ウェブ サービスのツール」を参照してください。
- AWSAWS Tools for Windows PowerShell - 詳細については、「AWS Tools for Windows PowerShell ユーザーガイド」を参照してください。

MediaConnect の料金

他の AWS 製品と同様、MediaConnect を使用するための契約や最低契約金は必要ありません。

トランスポートストリームフローの場合、フローの実行中は 1 時間あたりの料金が課金され、インターネットに配信される出力には GB あたりの料金が課金されます。また、同じリージョン内の入力データまたは出力データには GB 単位の料金が課金されます。一般に、ビットレートフローが高いほど、1 時間あたりの料金も高くなります。

CDI フローの場合、フローの実行中は 1 時間あたりの料金が請求され、いずれかの宛先に出力が配信されると 1 時間あたりの料金が請求されます。実行中のフローレートと出力ごとのレートは、動画のサイズに応じて変化します。SD 出力は UHD 出力よりも安価で、HD 出力よりも安価です。

両方のタイプのフローの詳細については、「AWS Elemental MediaConnect の料金表」を参照してください。

MediaConnect のリージョンとエンドポイント

アプリケーションのデータレイテンシーを減らすため、AWS Elemental MediaConnect ではリージョンのエンドポイントからリクエストを実行できます。

```
https://mediaconnect.<region>.amazonaws.com
```

MediaConnect を使用できる AWS リージョンの完全なリストを表示するには、「AWS 全般のリファレンス」の「AWS Elemental MediaConnect エンドポイントとクォータ」を参照してください。

AWS Elemental MediaConnect のユースケース

このセクションでは、AWS Elemental MediaConnect を実装して AWS クラウドやさらにそれを超えてコンテンツを配信するさまざまな方法を理解するのに役立つ、シンプルなビジネスユースケースを紹介します。このセクションのユースケースでは、お客様が求めている結果を得るために MediaConnect API を使用する方法の詳細は言及せず、わかりやすく説明しています。

MediaConnect の実装は、ユースケースによって異なります。

- コントリビューションでは、MediaConnect を使用してオンプレミスのエンコーダーから AWS クラウドにコンテンツを取り込みます。取り込むコンテンツのタイプに応じて、トランスポートストリームフローまたは CDI フローを作成できます。
- ディストリビューションでは、MediaConnect を使用してコンテンツをさまざまな地域に配信します。
- エンタイトルメントでは、MediaConnect を使用してコンテンツを他の AWS アカウントと共有します。
- レプリケーションとモニタリングでは、MediaConnect を使用して複数の宛先に動画を配信し、複数の動画信号をリアルタイムでモニタリングできるようにします。

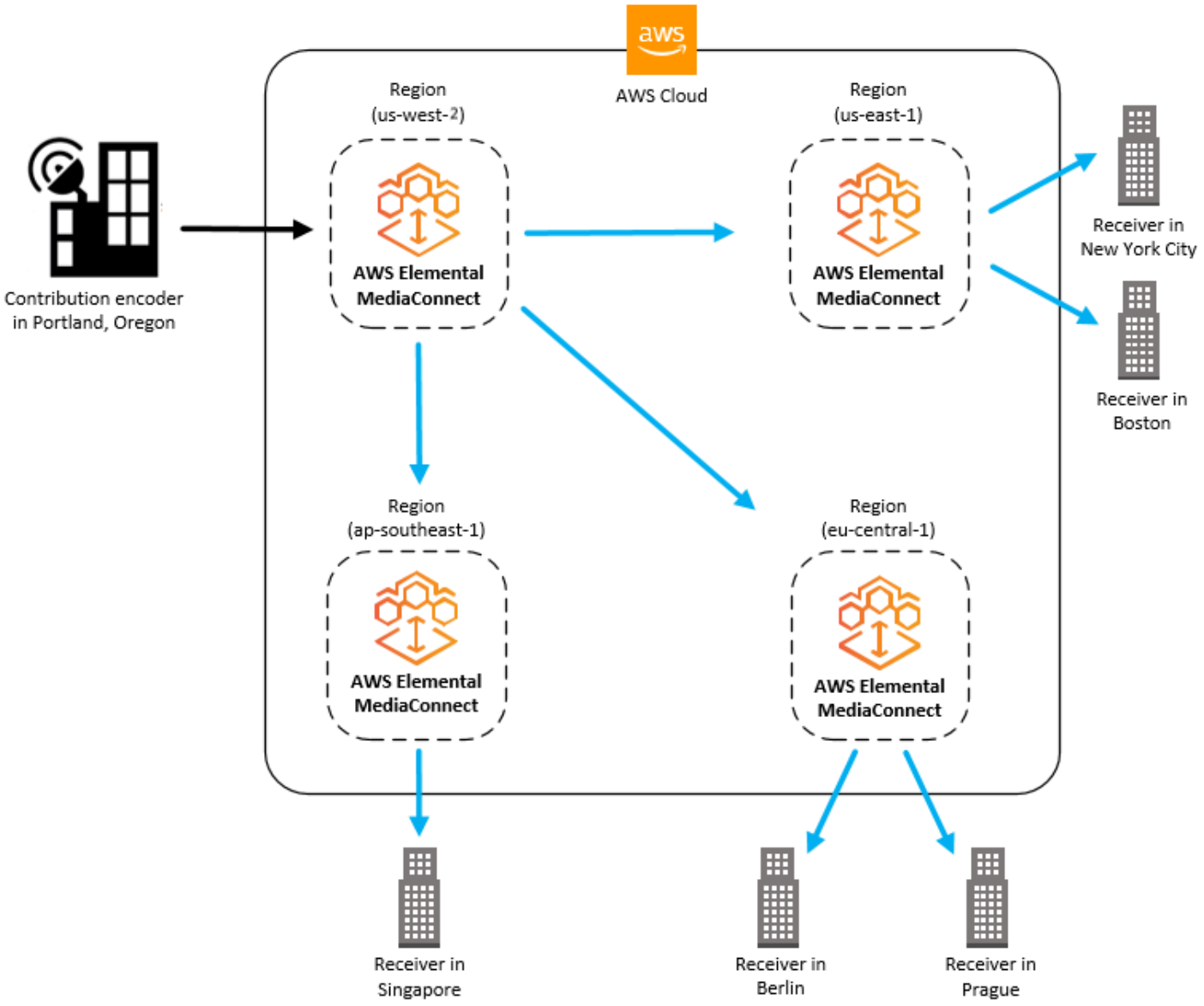
トピック

ユースケース: ディストリビューション

AWS Elemental MediaConnect を使用して、コンテンツをさまざまな地域に配信できます。たとえば、オンプレミスのコントリビューションエンコーダーがオレゴン州ポートランドにあり、レシーバーが世界各地に分散しているとします。(レシーバーとは、フローからコンテンツを受信するあらゆるエンティティです。これには、クラウド内のエンコーダーや受信施設のオンプレミスエンコーダー、または別の MediaConnect フローなどが考えられます。) 最初の MediaConnect フローは、エンコーダに最も近い物理的な AWS リージョンである us-west-1 リージョンで設定します。コンテン

ツが AWS クラウドに保存されたら、レシーバーにより近いリージョンにある他の MediaConnect フローに送信します。

次の図は、AWS クラウドの MediaConnect にコンテンツをアップロードするオレゴン州ポートランドにあるオンプレミスのコントリビューションエンコーダーを示しています。このフローには、異なる AWS リージョンの他のフローにコンテンツを送信する 3 つの出力があります。これらの 2 次フローは、世界中のさまざまな都市に設置されたレシーバーにより近いフローです。

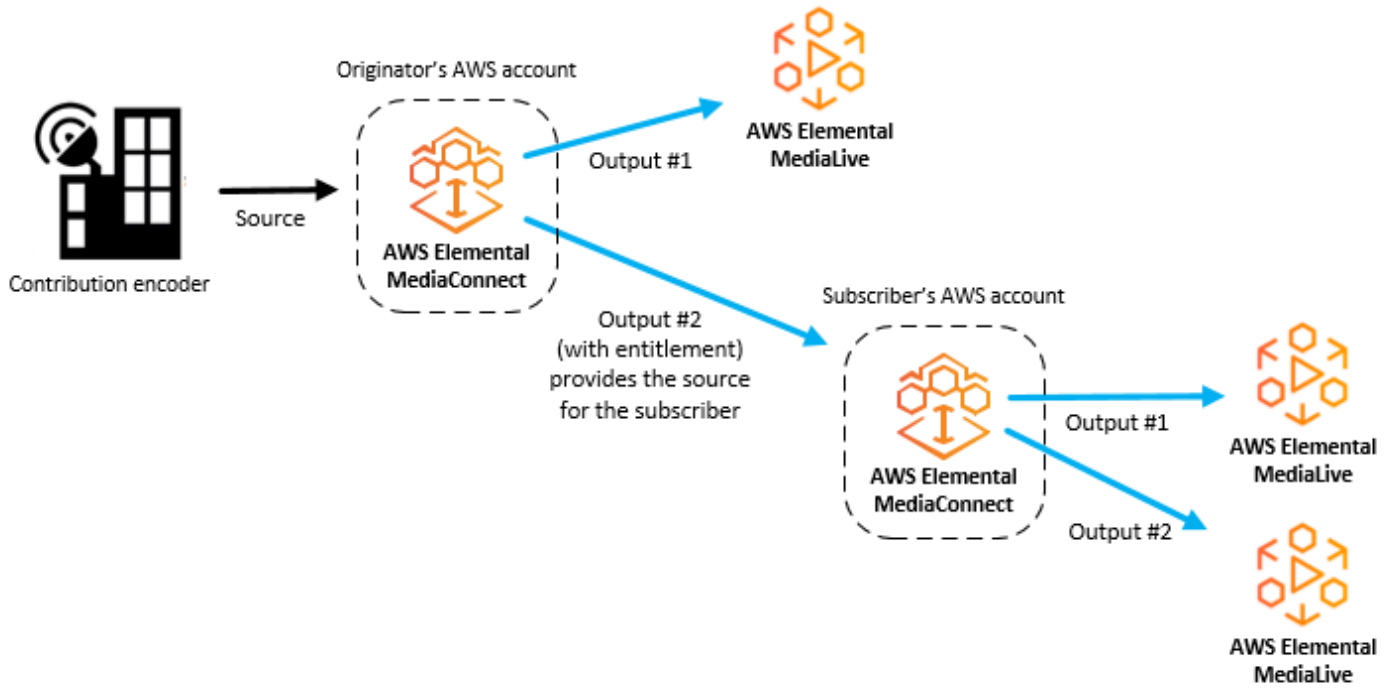


ユースケース: エンタイトルメント

エンタイトルメントにより、ある AWS アカウント所有者がトランスポートストリームフロー内のコンテンツを他の AWS アカウント所有者と共有できます。たとえば、あるスポーツ会社がフロー (野球の試合) を地元のテレビ局と共有したいとします。スポーツ放送局 (発信者) は、地元のテレビ局 (サブスクライバー) がアクセスできるように野球の試合のフローにエンタイトルメントを作成します。地元のテレビ局は、野球の試合フローからの出力をソースとして使用して AWS Elemental MediaConnect フローを作成します。

サブスクライバーは、発信者のフローと同じリージョンで MediaConnect にフローを設定する必要があります。

次の図は、トランスポートストリームフロー内のコンテンツを別の AWS サブスクライバーと共有する方法を示しています。発信者のフローの出力は、サブスクライバーのフローのソースとして使用できます。



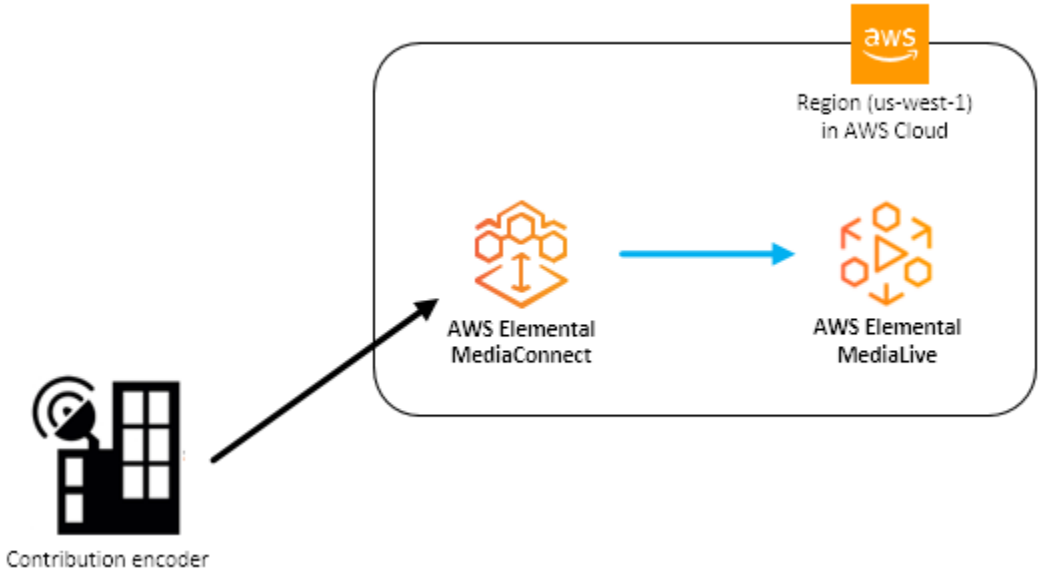
ユースケース: トランスポートストリームフローへのコントリビューション

AWS Elemental MediaConnect を使用して、オンプレミスのコントリビューションエンコーダーからクラウドにコンテンツを取り込むことができます。AWSMediaConnect フローのソースはオンプ

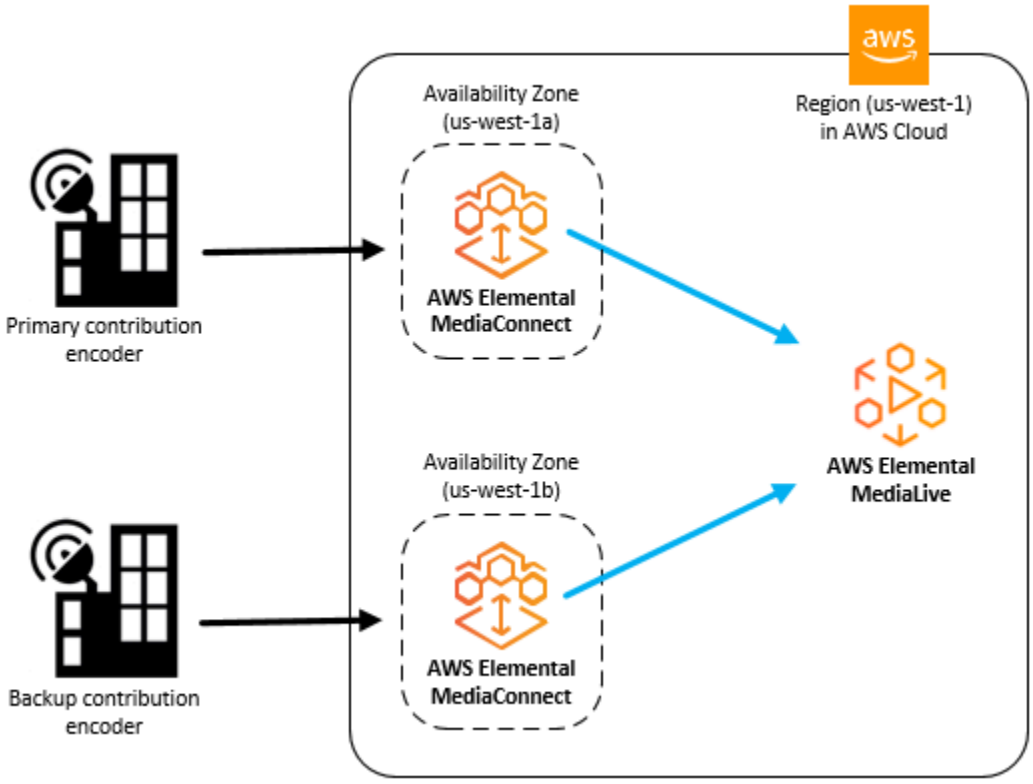
レミスのコントリビューションエンコーダーから取得され、出力先はクラウド内のエンコーダー (AWS Elemental MediaLive など) です。ソースコンテンツが圧縮されていない場合は、CDI ワークフローを使用できます。

冗長性を保つため、クラウドエンコーダーに向けた出力が 2 つになるようにフローを設定できます。もう 1 つの冗長設定には、2 つのオンプレミスコントリビューションエンコーダー (プライマリとバックアップ) があり、それぞれが異なる MediaConnect フローにコンテンツを送信します。その後、各フローからの出力は同じクラウドエンコーダーに向けられます。

次の図は、AWS クラウドの MediaConnect にコンテンツをアップロードするオンプレミスのコントリビューションエンコーダーを示しています。フロー出力は MediaLive チャネルに向けられます。



次の図は、同じコンテンツを AWS クラウドのMediaConnect にアップロードする 2 つのオンプレミスコントリビューションエンコーダー (プライマリとバックアップ) を示しています。2 つのフローがあり、それぞれに 1 つの出力があります。どちらの出力も単一の MediaLive チャンネルに向けられます。



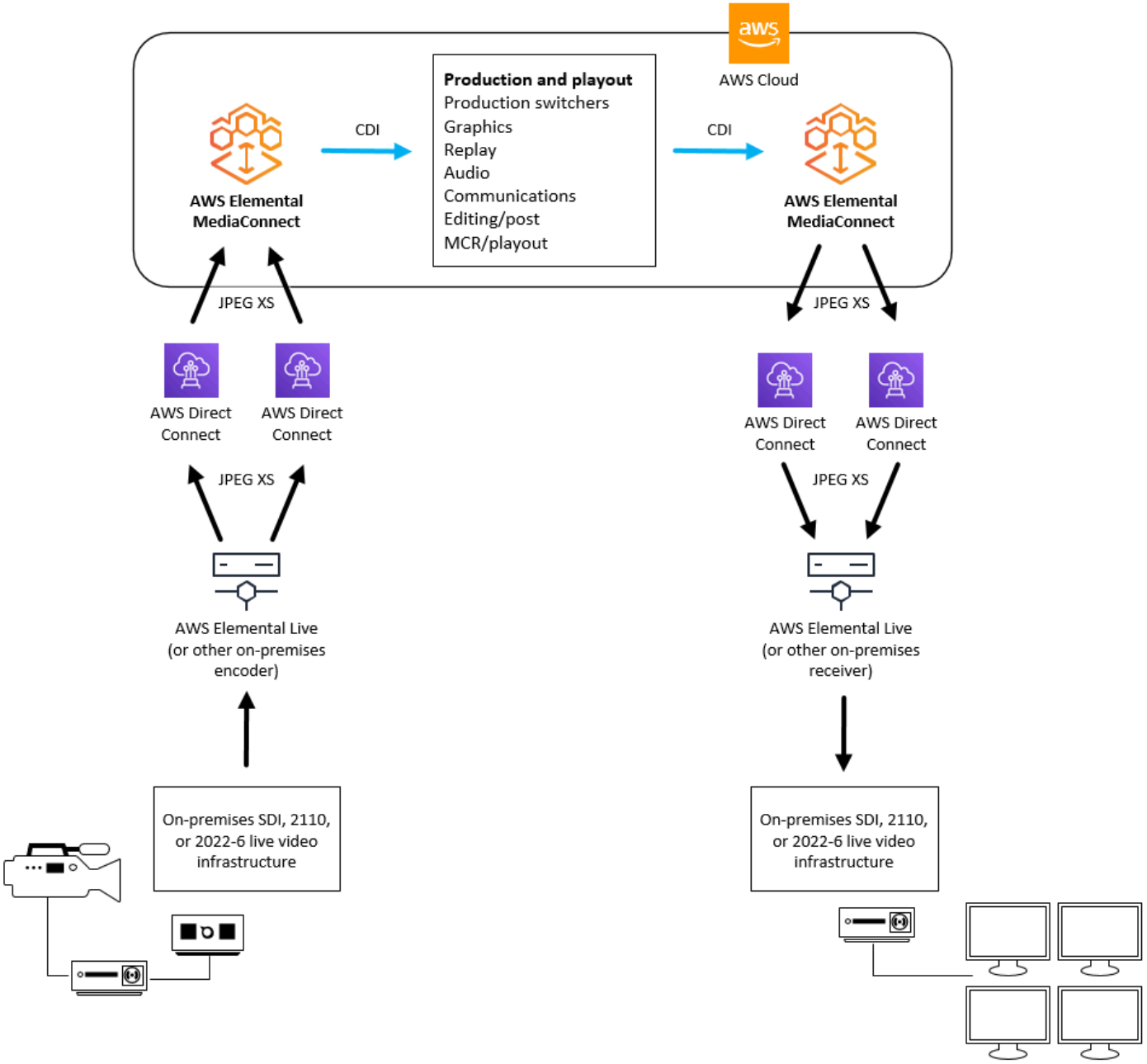
ユースケース: CDI フローへのコントリビューション

AWS Elemental MediaConnect と Direct Connect を使用すると、オンプレミスのライブ動画ネットワーク (SDI、2022-6、または 2110) を VPC ライブ動画ネットワーク (CDI) にブリッジできます。MediaConnect は JPEG XS コーデックを使用して、Direct Connect ネットワーク帯域幅を大幅に削減します。MediaConnect は、動画、オーディオ、およびメタデータの転送に SMPTE 2110 規格 (パート 22、30、40) をサポートしています。MediaConnect はコンテンツを CDI ストリームに変換するので、AWS Elemental MediaLive などのクラウド内の他のサービスですぐに使用できるようになります。クラウド VPC コンテンツをオンプレミスのネットワークに配信し直す準備ができたら、MediaConnect を使用して CDI ストリームを変換し、SMPTE 2110 規格 (パート 22、30、40) で転送することができます。

冗長性を保つため、オンプレミス設定と AWS クラウド間でコンテンツを転送するときは、Direct Connect に 2 つの接続を設定します。必ず、MediaConnect フローに合わせて AWS Elemental Live アプライアンスを設定してください。アプライアンスの設定について詳しくは、「AWS Elemental Liveユーザーガイド」の「SMPTE 2110の入力と出力」を参照してください。

> **Note**
>
> CDI 出力はアベイラビリティーゾーン間の転送をサポートしていないため、別のアベイラビリティーゾーンにコンテンツを送信する場合は ST 2110 JPEG XS 出力を使用してください。

次の図は、オンプレミスのライブ動画インフラストラクチャと AWS クラウドをつなぐワークフローを示しています。



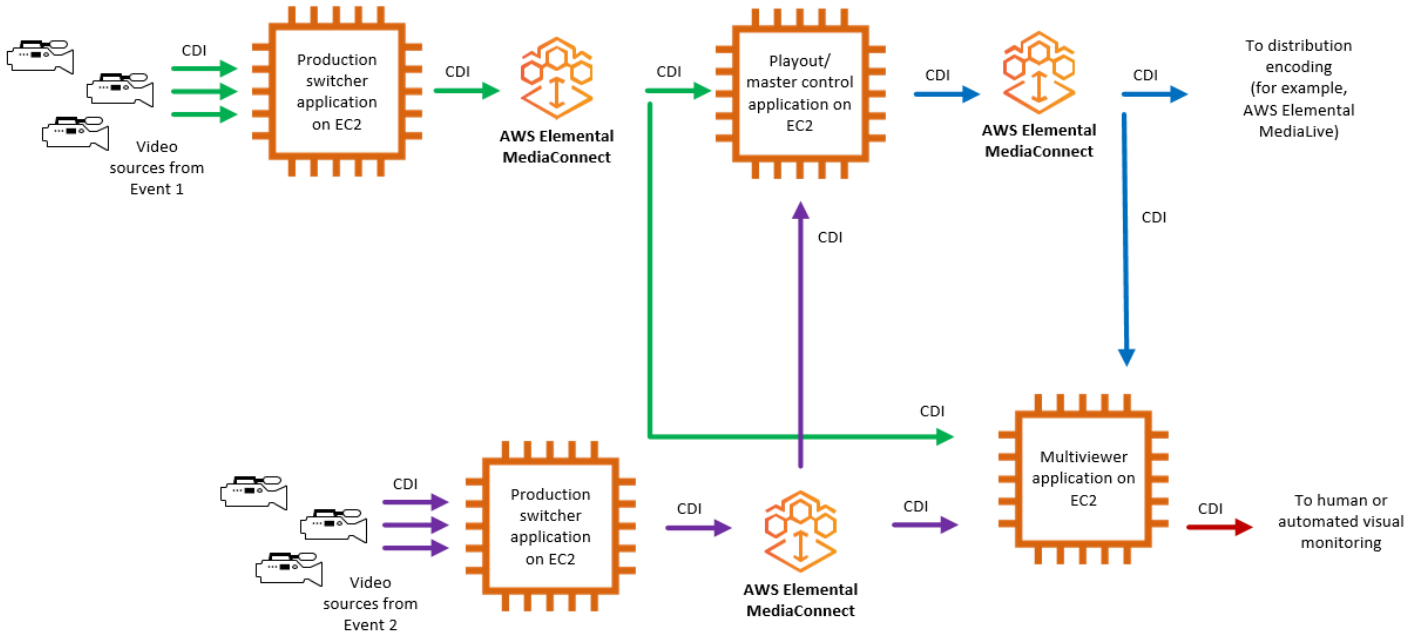
ユースケース: CDI フローのレプリケーションとモニタリング

AWS Elemental MediaConnect を使用すると、動画をレプリケーションして複数の宛先に配信し、複数のビデオ信号をリアルタイムでモニタリングできます。

たとえば、異なる会場で行われている複数のライブイベントの間で切り替えて、1 つの出力ブロードキャストを作成できます。MediaConnect CDI ワークフローを使用すると、複数のプロダクションスイッチャーからの出力をマスターコントロールスイッチャーとマルチビューア アプリケーションに

送信できます。別の CDI フローを使用して、ディストリビューションエンコーダー (AWS Elemental MediaLive など) に最終出力を送信したり、マルチビューア アプリケーションに送信したりできます。制作チームはマルチビューアーからの出力を受け取り、これにより複数のビデオ信号をリアルタイムでモニタリングできます。

次の図は、MediaConnect CDI ワークフローを使用して動画をレプリケーションし、複数の宛先に配信する方法を示しています。複数のイベントからの動画コンテンツから 1 つの出力ブロードキャストを作成できるほか、複数の信号からの出力を送信してリアルタイムでモニタリングすることもできます。



AWS Elemental MediaConnect のセットアップ

AWS Elemental MediaConnect の使用を開始する前に、 にサインアップし AWS （ AWS アカウントをお持ちでない場合 ）、MediaConnect へのアクセスを許可する IAM ユーザーとロールを作成する必要があります。これには、自分自身の IAM ロールを作成することが含まれます。暗号化を使用してコンテンツを保護する場合は、暗号化キーを に保存し AWS Secrets Manager、Secrets Manager アカウントからキーを取得するアクセス許可を MediaConnect に付与する必要があります。

このセクションでは、AWS Elemental MediaConnect にアクセスするユーザーおよびロールの設定に必要なステップを詳しく説明します。MediaConnect 向けの Identity and Access Management に関する背景と追加情報については、「the section called “Identity and Access Management”」を参照してください。

トピック

管理者以外のロールの作成

アカウントの管理者グループのユーザーは、そのアカウントのすべての AWS サービスとリソースにアクセスできます。すべての AWS リソースへの直接アクセスを許可することは、最小特権のアクセス許可をユーザーに適用するというベストプラクティスに反します。このセクションでは、アクセス許可が AWS Elemental MediaConnect に制限されたロールを作成する方法について説明します。このセクションでは、ユーザーがそのロールを引き受け、安全で一時的な認証情報を付与する方法についても説明します。

トピック

ステップ 1: 管理者以外のポリシーを作成する

AWS Elemental MediaConnect 向けに、読み取り/書き込みアクセス権を付与するポリシーと、読み取り専用アクセス権を付与するポリシーの 2 つのポリシーを作成します。ポリシーごとに以下の

ステップを 1 回のみ実行します。その後、これらのポリシーをロールにアタッチします。その後、ユーザーがこれらのロールを一時的に引き受け、MediaConnect へのアクセスを許可することができます。

ポリシーを作成するには

1. AWS アカウント ID またはアカウントエイリアス、および管理者ユーザーの認証情報を使用して、IAM コンソールにサインインします。
2. コンソールのナビゲーションペインで、[Policies] (ポリシー) を選択します。
3. ポリシー ページで、`MediaConnectAllAccess` という名前のポリシーを作成します。このポリシーは、AWS Elemental MediaConnect のすべてのリソースに対するすべてのアクションを許可します。

   a. [Create policy] (ポリシーの作成) を選択します。

   b. [JSON] タブを選択し、以下のポリシーを貼り付けます。

      JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
}
```

このポリシーでは、AWS Elemental MediaConnect のすべてのリソースに対するすべてのアクションを許可します。

c. [Next: Tags (次へ: タグ)] を選択します。

d. [次へ: レビュー] を選択します。

e. 確認と作成ページで、ポリシー名に と入力し**MediaConnectAllAccess**、ポリシーの作成を選択します。

4. ポリシー ページで、`MediaConnectReadOnlyAccess` という名前の AWS Elemental MediaConnect の読み取り専用ポリシーを作成します。

a. [Create policy] (ポリシーの作成) を選択します。

b. [JSON] タブを選択し、以下のポリシーを貼り付けます。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:List*",
                "mediaconnect:Describe*"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
}
```

c. [Next: Tags] (次へ: タグ) を選択します。

d. [次へ: レビュー] を選択します。

e. 確認と作成ページで、ポリシー名に と入力し**MediaConnectReadOnlyAccess**、ポリシーの作成を選択します。

ステップ 2: 管理者以外のロールを作成する

ユーザーごとに個別のポリシーをアタッチするのではなく、ポリシーごとにロールを作成してユーザーがロールを引き受けることができます。以下の手順を使用して、2 つのロールを作成します。1

つは MediaConnectAllAccess ポリシー用、もう 1 つは MediaConnectReadOnlyAccess ポリシー用です。

ロールを作成するには

1. IAM コンソールのナビゲーションペインで [ロール] を選択します。
2. ロール ページで、`MediaConnectAllAccess` ポリシーを使用して管理者ロールを作成します。
   a. [ロールの作成] を選択してください。
   b. 信頼できるエンティティの選択 セクションで、AWS アカウント を選択します。
   c. AWS アカウント セクションで、このロールを引き受けるユーザーのアカウントを選択します。
      i. 第三者がこのロールにアクセスする場合は、外部 ID が必要 を選択するのがベストプラクティスです。外部 ID の詳細については、「IAM ユーザーガイド」の「サードパーティーへのアクセスに外部 ID を使用する」を参照してください。
      ii. 多要素認証 (MFA) を必要とするのがベストプラクティスです。[MFA が必要] の横にあるチェックボックスを選択できます。MFA の詳細については、「IAM ユーザーガイド」の「多要素認証 (MFA)」を参照してください。
   d. 次へ を選択して 権限の追加 セクションに移動します。
   e. アクセス権限ポリシー セクションで、「ステップ 3a: ポリシーを作成する」の手順で作成した MediaConnectAllAccess ポリシーを選択します。
   f. このグループに正しいポリシーが追加されていることを確認し、次へ を選択します。
   g. 名前、確認、作成 セクションで、ロールに `MediaConnectAdmins` という名前を付けます。(オプション) ロールの説明を追加します。[Create role] (ロールの作成) を選択します。
3. ロール ページで、`MediaConnectReadOnlyAccess` ポリシーを使用して管理者ロールを作成します。
   a. [ロールの作成] を選択してください。
   b. 信頼できるエンティティの選択 セクションで、AWS アカウント を選択します。
   c. AWS アカウント セクションで、このロールを引き受けるユーザーのアカウントを選択します。

i. 第三者がこのロールにアクセスする場合は、外部 ID が必要 を選択するのがベストプラクティスです。外部 ID の詳細については、「IAM ユーザーガイド」の「サードパーティーへのアクセスに外部 ID を使用する」を参照してください。

ii. 多要素認証 (MFA) を必要とするのがベストプラクティスです。[MFA が必要] の横にあるチェックボックスを選択できます。MFA の詳細については、「IAM ユーザーガイド」の「多要素認証 (MFA)」を参照してください。

d. 次へ を選択して 権限の追加 セクションに移動します。

e. アクセス権限ポリシー セクションで、ステップ 3a: ポリシーを作成する の手順で作成した MediaConnectReadOnlyAccess ポリシーを選択します。

f. このグループに正しいポリシーが追加されていることを確認し、次へ を選択します。

g. 名前、確認、作成 セクションで、ロールに `MediaConnectReaders` という名前を付けます。(オプション) ロールの説明を追加します。[Create role] (ロールの作成) を選択します。

ステップ 3: ロールを引き受ける

ポリシーを作成してそのポリシーをロールにアタッチしたら、ユーザーはそのロールを引き受け、MediaConnect への安全で一時的なアクセスを許可する必要があります。

ロールを引き受ける許可をユーザーに付与する方法と、ユーザーがコンソールまたは AWS CLIからロールに切り替える方法については、以下のリソースをご覧ください。

- ロールを切り替えるアクセス許可をユーザーに付与する: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_permissions-to-switch.html
- ロール (コンソール) の切り替え: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html
- ロール (AWS CLI) の切り替え: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-cli.html

(オプション) 暗号化の設定

暗号化によりコンテンツを不正使用から保護できます。ソースが暗号化されている場合、AWS Elemental MediaConnect はそのソースを復号化できます。さらに、このサービスは出力と使用権限を暗号化できます。AWS Elemental MediaConnect には、コンテンツの暗号化に 2 つのオプションがあります。1 つはスタティックキーで、もう 1 つは Secure Packager and Encoder Key Exchange

(SPEKE) です。暗号化を設定する手順は、選択した暗号化のタイプによって異なります。詳細については次を参照してください:

- AWS Elemental MediaConnect を使用したスタティックキー暗号化のセットアップ
- AWS Elemental MediaConnect を使用した SPEKE 暗号化の設定

AWS Elemental MediaConnect の使用を開始する

この「開始方法」チュートリアルでは、AWS Elemental MediaConnect を使用してフローを作成し、共有する方法を説明します。このチュートリアルは、以下のすべてを実行したいというシナリオに基づいています。

- ニューヨーク市で行われているアワードショーのライブビデオストリームを取り込んでください。
- AWS アカウントを持っておらず、コンテンツをオンプレミスエンコーダーに送信したいと考えているボストンの関連会社にビデオを配信します。
- AWS アカウントを使ってローカルの 3 局に動画を配信したいと考えているフィラデルフィアの関連会社にビデオを共有してください。

トピック

前提条件

AWS Elemental MediaConnectを使用する前に、MediaConnect コンポーネントへのアクセス、表示、編集を行うためのアカウントと適切な権限が必要です。「AWS Elemental MediaConnect のセットアップ」の手順を完了してから、このチュートリアルに戻ってください。

ステップ 1: AWS Elemental MediaConnect にアクセスする

AWS アカウントを設定し、IAM ロールを作成したら、AWS Elemental MediaConnect のコンソールにサインインします。

AWS Elemental MediaConnect へのアクセス

- MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。

ステップ 2: フローを作成する

まず、AWS Elemental MediaConnect フローを作成して、オンプレミスのエンコーダーから AWS クラウドにビデオを取り込みます。このチュートリアルでは、以下の詳細を使用します。

- フロー名：AwardsNYCShow
- ソース名：AwardsNYCSource
- ソースプロトコル：Zixi プッシュ
- Zixi ストリーム ID：ZixiAwardsNYCFeed
- コンテンツを送信する CIDR ブロック：10.24.34.0/23
- ソース暗号化：なし

フローを作成するには

1. フロー ページで フローを作成 を選択します。
2. [詳細] セクションで、[名前] に「**AwardsNYCShow**」と入力します。
3. [アベイラビリティーゾーン] で、[任意] を選択します。
4. [ソース] セクションで、[ソースタイプ] として [標準ソース] を選択します。
5. [名前] に **AwardsNYCSource** と入力します。
6. [プロトコル] には [Zixi プッシュ] を選択します。AWS Elemental MediaConnect がインジェストポートの値を入力します。
7. [ストリーム ID] には、**ZixiAwardsNYCFeed** を入力します。
8. [許可リスト CIDR] には、**10.24.34.0/23** を入力します。
9. [Create flow (フローの作成)] を選択します。

ステップ 3：出力を追加します

ボストンのアフィリエイトにコンテンツを送信するには、フローに出力を追加する必要があります。この出力により、ボストンの関連会社のオンプレミスエンコーダーにビデオが送信されます。このチュートリアルでは、以下の詳細を使用します。

- 出力名：AwardsNYCOutput
- 出力プロトコル：Zixi プッシュ
- Zixi ストリーム ID：ZixiAwardsOutput
- ボストン関連会社のオンプレミスエンコーダの IP アドレス：198.51.100.11
- 出力暗号化：なし

出力を追加するには

1. [フロー] ページで、**AwardsNYCShow** フローを選択します。
2. [Outputs] タブを選択します。
3. [出力の追加] を選択します。
4. [名前] に **AwardsNYCOutput** と入力します。
5. [出力タイプ] で、[標準出力] を選択します。
6. [プロトコル] には [Zixi プッシュ] を選択します。
7. [ストリーム ID] には、**ZixiAwardsOutput** を入力します。
8. [宛先 IP アドレス] には、**198.51.100.11** を入力します。
9. [Port (ポート)] に「**1024**」と入力します。
10. [出力の追加] を選択します。

ステップ 4：エンタイトルメントの付与

フィラデルフィアの関連会社が AWS Elemental MediaConnect フローのソースとしてコンテンツを使用できるようにするには、エンタイトルメントを付与する必要があります。このチュートリアルでは、以下の詳細を使用します。

- エンタイトルメント名：PhillyTeam
- フィラデルフィア関連会社の AWS アカウント ID：222233334444
- 出力暗号化：なし

エンタイトルメントを付与するには

1. [実験] タブを選択します。

2. [エンタイトルメントを付与] を選択します。
3. [名前] に **PhillyTeam** と入力します。
4. [サブスクライバー] には、**222233334444** を入力します。
5. [エンタイトルメントを付与] を選択します。

ステップ 5：関連会社と詳細情報の共有

ボストン関連会社用の出力とフィラデルフィア関連会社用のエンタイトルメントを含む AWS Elemental MediaConnect フローを作成したので、フローの詳細を伝える必要があります。

ボストンの関連会社は、オンプレミスエンコーダでフローを受信します。ビデオストリームの送信先の詳細はボストンの関連会社から提供されているので、他の情報を提供する必要はありません。フローを開始すると、コンテンツはフローの作成時に指定した IP アドレスに送信されます。

フィラデルフィアの関連会社は、自社のフローをソースとして使用して、独自の AWS Elemental MediaConnect フローを作成する必要があります。フィラデルフィアの関連会社に以下の情報を指定する必要があります。

- エンタイトルメント ARN：この値は、AwardsNYCShow フロー詳細ページの [エンタイトルメント] タブで確認できます。
- リージョン：これは AwardsNYCShow フローを作成した AWS リージョンです。

ステップ 6: クリーンアップする

不要な課金を回避するには、すべての不要なフローを削除してください。フローを削除するには、フローを停止する必要があります。

フローを止めるには

1. [フロー] ページで、**AwardsNYCShow** フローを選択します。

   AwardsNYCShow フローの詳細ページが表示されます。
2. [Stop] (停止) を選択します。

フローを消去する方法

1. AwardsNYCShow フローの詳細ページで、[削除] を選択します。

確認メッセージが表示されます。

2. [フローの削除] を選択します。

AWS Elemental MediaConnect におけるフロー

フローは、ソースと 1 つ以上の送信先間のトランスポートです。フローを作成するときは、ソース、名前、アベイラビリティーゾーンを指定します。フローを作成したら、コンテンツの送信先と転送方法を示す出力を追加できます。

MediaConnect では、2 タイプのフローがサポートされます。

- トランスポートストリームフロー は、マックスされた圧縮コンテンツ (オーディオ、動画、および補助データを組み合わせたもの) を 1 つのストリームに転送します。その品質は、消費者向けデバイスに配信される最終的なエンコードを作成するためのソースとして使用できるほど高品質です。出力を追加して、コンテンツの送信先と転送方法を指定できます。

  コンテンツを別の AWS アカウントと共有する使用権限を付与できます。その後、サブスクライバーアカウントのユーザーは、自分のフローをソースとして使用して新しい MediaConnect フローを作成できます。これが起きると、サービスはサブスクライバーのフローをフィードするストリームを表す出力をフローに生成します。

  フロー上の出力と使用権限の数を管理することが重要です。各トランスポートストリームフローの出力は 50 個までです。1 つのフローで最大 50 個の使用権限を付与できますが、それぞれの使用権限によって出力が生成されます。たとえば、**BasketballGame** という名前のフローを作成し、コンテンツをオンプレミスのエンコーダーに送信する 40 の出力を追加するとします。また、コンテンツを他の AWS アカウントと共有するための使用権限を 30 個付与します。サブスクライバーが **BasketballGame** をソースとして使用してフローを作成すると、サービスはそれらのサブスクライバーごとに新しい出力を生成します。最初の 10 人のサブスクライバーがフローを作成すると、**BasketballGame** フローの最大出力数 (作成した元の出力は 40 個、購読するフロー用にサービスが作成した出力がさらに 10 個) に達します。11 人目のサブスクライバーが **BasketballGame** をソースとして使用してフローを作成しようとすると、サービスはエラーを返します。
- CDI フロー は、高品質の非圧縮コンテンツや軽く圧縮されたコンテンツを AWS クラウドに出入りさせます。JPEG XS を使用して軽く圧縮されたコンテンツを転送するように CDI フローを設定できます。コンテンツは、オーディオ、動画、または補助データ用に別々のメディアストリームに逆多重化されます。各 CDI フローでは、ソースに複数のメディアストリームを使用し、出力ごとに複数のメディアストリームを使用できます。MediaConnect は AWS Cloud Digital Interface (AWS CDI) ネットワーク技術を使用して、SMPTE 2110、パート 22 トランスポート標準に準拠したコンテンツを転送します。

トピック

フローの作成

フローは、1 つ以上のソースと 1 つ以上の出力または使用権限の間の接続です。

フローの作成に使用する方法は、作成するフローの種類とソース内のコンテンツの種類によって異なります。

- 標準ソースでのトランスポートストリームフロー — VPC ソースでも使用権限のあるソースでもない任意のソースからのコンテンツを使用します。
- エンタイトルメントのあるソースを持つトランスポートストリームフロー – アカウントにエンタイトルメントを付与 AWS アカウント した別の が所有するコンテンツを使用します。
- VPC ソースでのトランスポートストリームフロー — 設定した VPC からの圧縮コンテンツを使用します。
- CDI フロー — 設定した VPC からの非圧縮コンテンツを使用します。

> **Note**
>
> フェイルオーバー用の冗長ソースを使用するトランスポートストリームフローを作成する場合は、いずれかのソースを使用してフローを作成します。フローが作成されたら、もう 1 つのソースを追加します。MediaConnect は両方のソースをプライマリソースとして扱うため、最初にフローを作成するときにどちらを指定してもかまいません。フローに使用権限のあるソースが使用されている場合、2 つ目のソースを追加することはできません。CDI ワークフローの冗長性を確保するには、2 つの別個のフローを作成します。

標準ソースを使用するトランスポートストリームフローの作成

トランスポートストリームフローは、圧縮されたコンテンツを 1 つのストリームに多重化して転送します。

フローは、コンテンツが VPC (VPC ソース) または別の AWS アカウント (使用権限のあるソース) 以外の場所から送信される場合に、標準ソースを使用します。

前提条件

開始する前に、次のステップを完了していることを確認してください。

暗号化設定 (必要な場合)

フローのソースで暗号化が必要な場合は、暗号化を設定する必要があります。

NDI® 設定 (NDI ユースケースのみ)

開始する前に、NDI 出力のドキュメントを確認して、この機能について理解しておくことをお勧めします。

フローに NDI 出力を追加する場合は、ネットワークに NDI 検出サーバーがプロビジョニングされた VPC が必要です。MediaConnect はこれらのサーバーに接続しますが、自動的には作成されません。

- VPCs、AWS CloudFormation VPC テンプレートを使用して、パブリックサブネットとプライベートサブネットを持つ VPC を自動的に作成できます。Amazon VPC の詳細については、「Amazon VPC ユーザーガイド」を参照してください。
- NDI 検出サーバーのデプロイの場合、 は、インストールと設定のベストプラクティスなど AWS CloudFormation、 を使用して複数のアベイラビリティーゾーンにまたがる自動セットアップに関するガイダンス AWS を提供します。手順については、「ブロードキャストワークフロー用の NDI 検出サーバーのセットアップ」を参照してください。
- 自己参照進入ルールと退出ルールを使用してセキュリティグループを設定することをお勧めします。その後、このセキュリティグループを、NDI サーバーが VPC 内で実行されている EC2 インスタンスにアタッチできます。このアプローチにより、VPC 内のコンポーネント間で必要なすべての NDI 通信が自動的に許可され、必要なすべてのネットワークトラフィックが許可されます。自己参照セキュリティグループルールの設定に関するガイダンスについては、「Amazon VPC ユーザーガイド」の「セキュリティグループの参照」を参照してください。

手順

標準ソース (コンソール) を使用するトランスポートストリームフローの作成

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで [フローを作成] を選択します。
3. [詳細] セクションの [名前] で、フローの名前を指定します。この名前は、このフローの ARN の一部になります。

   > **Note**
   >
   > MediaConnect では、同じ名前で複数のフローを作成できます。ただし、整理しやすいように、 AWS リージョン内では一意のフロー名を使用することをお勧めします。フローの作成後に、名前は変更できません。

4. [アベイラビリティーゾーン] で、フローのアベイラビリティーゾーンを選択します。冗長フローを設定する場合は、このオプションを使用します。それ以外の場合は、[任意] のままにしておくことができます。デフォルトのままにすると、サービスは現在の AWS リージョン内のアベイラビリティーゾーンをランダムに割り当てます。ソースが VPC からのものである場合、サービスは VPC サブネットのアベイラビリティーゾーンをフローに割り当てます。
5. 「フローサイズ」で、ユースケースに合ったサイズを選択します。フローサイズの詳細については、「フローサイズと機能」を参照してください。

   中フローの場合：

   - ステップ 6 に直接進んでください。

   大きなフローの場合：

   - フローに NDI 出力が必要ない場合は、ステップ 6 に直接進んでください。
   - フローに NDI 出力を追加する場合は、次のように NDI 設定を行います。
     1. フロー NDI サポートを Enabled に設定します。
     2. (オプション) NDI マシン名を入力します。
        - この名前は、フローが作成する NDI ソースを識別するのに役立つプレフィックスとして使用されます。たとえば、 と入力すると**MACHINENAME**、NDI ソースは **MACHINENAME** として表示されます(`ProgramName`)。

- 名前を入力しない場合、MediaConnect はプレフィックスとして一意の 12 文字の ID を生成します。この ID はフローの Amazon リソースネーム (ARN) から取得されるため、マシン名はフローリソースを参照します。

> **Tip**
>
> NDI ソースを作成するフローが複数ある場合、慎重に命名することが特に重要です。たとえば、100 個の NDI ソースを持つ本番環境では、STUDIO-A、、STUDIO-Bなどの明確でわかりやすいマシン名のプレフィックスが役立ちますNEWSROOM。

3. 最大 3 つの NDI 検出サーバーを追加します。サーバーごとに、次の情報を指定します。
   - 既存の NDI インフラストラクチャのサーバー IP アドレスを入力します。
   - VPC インターフェイスアダプターを選択して、ネットワークアクセスを制御します。
   - (オプション) ポート番号を指定します。これを空白のままにすると、MediaConnect は NDI Discovery サーバーのデフォルトである TCP-5959 を使用します。

> **Tip**
>
> 最大 3 つの検出サーバーを追加できます。複数の検出サーバーを持つことで信頼性が向上し、NDI ソースがネットワーク全体で検出可能になります。

6. ソースがどのプロトコルを使用するかを決定します。

> **Note**
>
> フェイルオーバー用の冗長ソースを指定する場合は、いずれかのソースを使用してフローを作成します。フローが作成されたら、ソースのフェイルオーバーを有効にするようにフローを更新し、2 つ目のソースをフローに追加します。MediaConnect は両方のソースをプライマリソースとして扱うため、最初にフローを作成するときにどちらを指定してもかまいません。

7. ソースタイプとプロトコルに基づく具体的な説明については、以下のタブから 1 つ選択してください

   RIST

   1. [ソース] セクションで、[ソースタイプ] として [標準ソース] を選択します。

2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。
3. [プロトコル] には、[RIST] を選択します。
4. [取り込みポート] には、フローが受信コンテンツをリッスンするポートを指定します。

> **Note**
>
> RIST プロトコルでは、エラー修正のために 1 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから +1 されたポートを予約します。例えば、出力にポート 4000 を指定すると、サービスにはポート 4000 と 4001 が割り当てられます。

5. [許可リスト CIDR] では、ソースへのコンテンツの提供が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、「RFC 4632」を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

6. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
7. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。1 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 2,000 ms を使用します。

RTP or RTP-FEC

1. [ソース] セクションで、[ソースタイプ] として [標準ソース] を選択します。
2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。

3. [プロトコル] には、[RTP] または [RTP-FEC] を選択します。
4. [取り込みポート] には、フローが受信コンテンツをリッスンするポートを指定します。

> **Note**
>
> RTP-FEC プロトコルでは、エラー修正のために 2 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから+ 2 および +4 されたポートを予約します。例えば、出力にポート 4000 を指定すると、サービスにはポート 4000、4002、および 4004 が割り当てられます。

5. [許可リスト CIDR] では、ソースへのコンテンツの提供が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、「RFC 4632」を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

6. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。

SRT listener

1. [ソース] セクションで、[ソースタイプ] として [標準ソース] を選択します。
2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。
3. [プロトコル] には、[SRT リスナー]を選択します。
4. [ソースの説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
5. [許可リスト CIDR ブロック] には、ソースへのコンテンツ提供を許可する IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、「RFC 4632」を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

6. [着信ポート] には、フローが着信コンテンツをリッスンするポートを指定します。
7. [ソースリスナーアドレス] には、MediaConnect が SRT 接続に使用するアドレスを入力します。アドレスは IP アドレスでもドメイン名でもかまいません。
8. [ソースの説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
9. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
10. [最小遅延] には、サービスに保持させたいバッファ (遅延) の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。10 ~ 15,000 ミリ秒の値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。

    SRT プロトコルは、接続の両側で最小レイテンシー設定を使用します。これら 2 つの値のうち大きい方を復旧レイテンシーとして使用します。送信ビットレートに復旧レイテンシーを掛けた値が受信バッファよりも高い場合、バッファはオーバーフローし、ストリームは で失敗する可能性がありますBuffer Overflow Error。SRT レシーバー側では、レシーバーバッファは SRTO_RCVBUF 値によって設定されます。レシーバーバッファのサイズは、フロー制御ウィンドウサイズ (SRTO_FC) 値によって制限されます。MediaConnect 側では、レシーバーバッファは最大ビットレート値に最小レイテンシー値を乗算して計算されます。SRT バッファの詳細については、SRT 設定ガイドラインを参照してください。
11. ソースが暗号化されている場合は、[有効化] セクションで [有効化] を選択し、次の操作を行います。

    a. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。

    b. シークレット ARN には、暗号化キーを保存するシークレットの作成時に が AWS Secrets Manager 割り当てた ARN を指定します。

SRT caller

1. [ソース] セクションで、[ソースタイプ] として [標準ソース] を選択します。
2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。
3. [プロトコル] には、[SRT コーラー] を選択します。
4. [ソースの説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
5. [ソースリスナーアドレス] には、MediaConnect が SRT 接続に使用するアドレスを入力します。アドレスは IP アドレスでもドメイン名でもかまいません。
6. [ソースリスナーポート] には、MediaConnect が SRT 接続に使用するポートを入力します。
7. [最大ビットレート] (オプション) には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
8. [最小遅延] には、サービスに保持させたいバッファ (遅延) の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。10 ~ 15,000 ミリ秒の値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。

   SRT プロトコルは、接続の両側で最小レイテンシー設定を使用します。これら 2 つの値のうち大きい方を復旧レイテンシーとして使用します。送信ビットレートに復旧レイテンシーを掛けた値が受信バッファよりも高い場合、バッファはオーバーフローし、ストリームは で失敗する可能性がありますBuffer Overflow Error。SRT レシーバー側では、レシーバーバッファは SRTO_RCVBUF 値によって設定されます。レシーバーバッファのサイズは、フロー制御ウィンドウサイズ (SRTO_FC) 値によって制限されます。MediaConnect 側では、レシーバーバッファは最大ビットレート値に最小レイテンシー値を乗算して計算されます。SRT バッファの詳細については、「SRT 設定ガイドライン」を参照してください。
9. [ストリーム ID] (オプション) には、ストリームの識別子を入力します。この識別子は、ストリームに関する情報を伝えるために使用できます。
10. ソースが暗号化されている場合は、[有効化] セクションで [有効化] を選択し、次の操作を行います。

    a. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。

b. シークレット ARN には、暗号化キーを保存するシークレットの作成時に が AWS Secrets Manager 割り当てた ARN を指定します。

Zixi push

1. [ソース] セクションで、[ソースタイプ] として [標準ソース] を選択します。
2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。
3. [プロトコル] には [Zixi プッシュ] を選択します。

> **Note**
>
> MediaConnect は、作成時に Zixi プッシュソースの受信ポートを割り当てます。2088 のポート番号が自動的に割り当てられます。

4. [許可リスト CIDR] では、ソースへのコンテンツの提供が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、「RFC 4632」を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

5. [ストリーム ID] には、Zixi フィーダーに設定されているストリーム ID を指定します。

> **Important**
>
> このフィールドを空白のままにすると、サービスはソース名をストリーム ID として使用します。ストリーム ID は Zixi フィーダーに設定された値と一致する必要があるため、ソース名とまったく同じでない場合はストリーム ID を指定する必要があります。

6. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増

えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0 ~ 60,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。

7. ソースが暗号化されている場合は、[有効化] セクションで [有効化] を選択し、次の操作を行います。

   a. [復号化タイプ] には [静的キー] を選択します。

   b. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。

   c. シークレット ARN には、暗号化キーを保存するシークレットの作成時に が AWS Secrets Manager 割り当てた ARN を指定します。

   d. [復号化アルゴリズム] では、ソースの暗号化に使用された暗号化のタイプを選択します。

Zixi push for AWS Elemental Link UHD device

MediaConnect のソースとして AWS Elemental Link デバイスを使用するには、次の手順を使用して Zixi プッシュフローを作成する必要があります。Zixi プッシュフローを作成したら、MediaLive を使用して AWS Elemental Link デバイスを設定する必要があります。フローの作成後にプロセスを完了するには、次の MediaLive 設定手順「MediaLive ユーザーガイド」の「フロー内でのデバイスの使用」を参照してください。これらの手順を完了するには、MediaConnect と MediaLive の両方にアクセスできることを確認してください。

1. [ソース] セクションで、[ソースタイプ] として [標準ソース] を選択します。
2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。
3. [プロトコル] には [Zixi プッシュ] を選択します。

> **Note**
>
> MediaConnect は、作成時に Zixi プッシュソースの受信ポートを割り当てます。2088 のポート番号が自動的に割り当てられます。

4. [許可リスト CIDR ブロック] には、ソースへのコンテンツ提供を許可する IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、「RFC 4632」を参照してください。

> **Important**
>
> Link デバイスがインターネットへの接続に使用するパブリック IP アドレスの範囲がわかっている場合は、その CIDR ブロックを入力します。これは AWS Elemental Link デバイスの IP アドレスと同じではないことに注意してください。この情報を取得できない場合は、0.0.0.0/0 を使用して、考えられるすべての IP アドレスに対して開かれるように CIDR ブロックを設定できます。通常、インターネット全体 (0.0.0.0/0) に開かれる CIDR ブロックを割り当てることはベストプラクティスではありません。ただし、この方法を使用する必要がある場合、転送されるデータは AES-128 暗号化を使用して暗号化されます。

5. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0 ~ 60,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。最大レイテンシー値は、AWS Elemental Link デバイスに設定されているレイテンシー値と一致する必要があります。リンクデバイスのレイテンシーの設定については、「AWS Elemental MediaLive ユーザーガイド」の「デバイスの設定」を参照してください
6. [復号化] では、有効化を選択し、次の操作を行います。
   a. [復号化タイプ] には [静的キー] を選択します。
   b. 復号アルゴリズムでは、AES-128 を選択します。AES-128 AWS Elemental Link が必要です。別のアルゴリズムを選択しないでください。
   c. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
   d. シークレット ARN には、暗号化キーを保存するシークレットの作成時に が AWS Secrets Manager 割り当てた ARN を指定します。

8. ソースモニタリング設定で、有効にするモニタリング機能を選択します。
   a. サムネイル状態をオンにして、コンソールでプレビューできるソースサムネイルを生成します。
   b. コンテンツ品質分析の状態をオンにして、次のオーディオおよびビデオ品質の問題を監視します。
      i. (オプション) ブラックフレームをオンにして、ストリーム内のブラックビデオフレームの期間を検出します。

ii. （オプション) フローズンフレームをオンにして、ストリーム内の変更されていないビデオフレームの期間を検出します。

iii. （オプション) サイレントオーディオをオンにして、ストリーム内のオーディオサイレンス時間を検出します。

iv. （オプション) 有効にするメトリクスごとに、10～60 秒の期間しきい値を設定します。デフォルト値は 30 秒です。

9. ページの下部で、[今すぐ作成] を選択します。

標準ソース (AWS CLI) を使用するトランスポートストリームフローの作成

1. 作成するフローの詳細を含む JSON ファイルを作成します。

   次の例では、ファイルのコンテンツを示します。

```
{
  "Name": "AwardsShow",
  "Outputs": [
    {
      "Destination": "198.51.100.5",
      "Description": "RTP output",
      "Name": "RTPOutput",
      "Protocol": "rtp",
      "Port": 5020
    }
  ],
  "Source": {
    "Name": "AwardsShowSource",
    "Protocol": "rtp-fec",
    "WhitelistCidr": "10.24.34.0/23"
  }
}
```

2. で AWS CLI、 `create-flow` コマンドを使用します。

```
aws mediaconnect create-flow --cli-input-json file://rtp.json --profile PMprofile
```

   戻り値の例を以下に示します。

```
{
  "Flow": {
```

```
    "EgressIp": "203.0.113.0",
    "AvailabilityZone": "us-east-1d",
    "Name": "AwardsShow",
    "Status": "STANDBY",
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
    "Source": {
            "SourceArn": "arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:AwardsShowSource",

            "Name": "AwardsShowSource",
            "IngestPort": 5000,
            "WhitelistCidr": "10.24.34.0/23",
            "IngestIp": "198.51.100.15",
            "Transport": {
                "Protocol": "rtp-fec",
                "MaxBitrate": 80000000
            }
        },
        "Entitlements": [],
        "Outputs": [
            {
                "Port": 5020,
                "Name": "AwardsShowOutput",
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:AwardsShowOutput",

                "Description": "RTP-FEC Output",
                "Destination": "198.51.100.5",
                "Transport": {
                    "Protocol": "rtp",
                    "SmoothingLatency": 0
                }
            }
        ]
    }
}
```

次のステップ

フローを作成したら、次のステップを実行してコンテンツの配信を開始します。

- MediaConnect フローがコンテンツを送信する場所を指定する出力を追加する
- 他のユーザーのユーザーがコンテンツを AWS アカウント サブスクライブできるようにする権限を付与します
- フローを開始してコンテンツ配信を開始する

その他のリソース

フローのソースモニタリングオプションの詳細については、このガイドの以下のページを参照してください。

- ソースビデオのサムネイルの表示
- でのコンテンツ品質分析によるモニタリング AWS Elemental MediaConnect

使用権限のあるソースを使用するトランスポートストリームフローの作成

トランスポートストリームフローは、圧縮されたコンテンツを 1 つのストリームに多重化して転送します。権限のあるソースは、別の AWS アカウントからのコンテンツです。

前提条件

- NDI® 設定 (NDI ユースケースのみ)

  NDI 出力のドキュメントを確認して、開始する前にこの機能について理解しておくことをお勧めします。

  フローに NDI 出力を追加する場合は、ネットワークに NDI 検出サーバーがプロビジョニングされた VPC が必要です。MediaConnect はこれらのサーバーに接続しますが、自動的には作成されません。

  - VPCs、AWS CloudFormation VPC テンプレートを使用して、パブリックサブネットとプライベートサブネットを持つ VPC を自動的に作成できます。Amazon VPC の詳細については、「Amazon VPC ユーザーガイド」を参照してください。
  - NDI 検出サーバーのデプロイの場合、 は、インストールと設定のベストプラクティスなど AWS CloudFormation、 を使用して複数のアベイラビリティーゾーンにまたがる自動セットアップに関するガイダンス AWS を提供します。手順については、「ブロードキャストワークフロー用の NDI 検出サーバーのセットアップ」を参照してください。
  - 自己参照進入ルールと退出ルールを使用してセキュリティグループを設定することをお勧めします。その後、このセキュリティグループを、NDI サーバーが VPC 内で実行されている EC2 イ

ンスタンスにアタッチできます。このアプローチにより、VPC 内のコンポーネント間で必要なすべての NDI 通信が自動的に許可され、必要なすべてのネットワークトラフィックが許可されます。自己参照セキュリティグループルールの設定に関するガイダンスについては、「Amazon VPC ユーザーガイド」の「セキュリティグループの参照」を参照してください。

手順

資格のあるソースを使用するトランスポートストリームフローを作成するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで [フローを作成] を選択します。
3. [詳細] セクションの [名前] で、フローの名前を指定します。この名前は、このフローの ARN の一部になります。

> **Note**
>
> MediaConnect では、同じ名前で複数のフローを作成できます。ただし、整理しやすいように、 AWS リージョン内では一意のフロー名を使用することをお勧めします。フローの作成後に、名前は変更できません。

4. アベイラビリティーゾーンでは、次のいずれかのオプションを選択します。

   - 任意の を選択 (推奨)
   - 特定のアベイラビリティーゾーンを選択する (冗長フローを設定する場合に役立ちます)

   デフォルト設定 (Any) を使用する場合、MediaConnect は現在の AWS リージョン内にアベイラビリティーゾーンをランダムに割り当てます。ソースが VPC からのものである場合、サービスは VPC サブネットのアベイラビリティーゾーンをフローに割り当てます。

> **Note**
>
> ソースが VPC に由来する場合、フローのアベイラビリティーゾーンは VPC サブネットのアベイラビリティーゾーンと一致する必要があります。これを [任意] のままにして、アベイラビリティーゾーンが正しく設定されていることをサービスに確認させることをお勧めします。

5. フローサイズで、ユースケースに合ったサイズを選択します。フローサイズの詳細については、「フローサイズと機能」を参照してください。

   中フローの場合：

   - ステップ 6 に直接進んでください。

   大きなフローの場合：

   - フローに NDI 出力が必要ない場合は、ステップ 6 に直接進んでください。
   - フローに NDI 出力を追加する場合は、次のように NDI 設定を行います。
     1. フロー NDI サポートを Enabled に設定します。
     2. （オプション) NDI マシン名を入力します。
        - この名前は、フローが作成する NDI ソースを識別するのに役立つプレフィックスとして使用されます。たとえば、 と入力すると**MACHINENAME**、NDI ソースは **MACHINENAME** として表示されます(`ProgramName`)。
        - 名前を入力しない場合、MediaConnect はプレフィックスとして一意の 12 文字の ID を生成します。この ID はフローの Amazon リソースネーム (ARN) から取得されるため、マシン名はフローリソースを参照します。

        > **Tip**
        > NDI ソースを作成するフローが複数ある場合、慎重に命名することが特に重要です。たとえば、100 個の NDI ソースを持つ本番環境では、`STUDIO-A`、、などの明確でわかりやすいマシン名のプレフィックスが役立ちます`STUDIO-BNEWSROOM`。

     3. 最大 3 つの NDI 検出サーバーを追加します。サーバーごとに、次の情報を指定します。
        - 既存の NDI インフラストラクチャのサーバー IP アドレスを入力します。
        - VPC インターフェイスアダプターを選択して、ネットワークアクセスを制御します。
        - （オプション) ポート番号を指定します。これを空白のままにすると、MediaConnect は NDI Discovery サーバーのデフォルトである TCP-5959 を使用します。

> **Tip**
>
> 最大 3 つの検出サーバーを追加できます。複数の検出サーバーを持つことで信頼性が向上し、NDI ソースがネットワーク全体で検出可能になります。

6. ソースセクションで、次の操作を行います。

   - ソースタイプで、使用権限のあるソースを選択します。
   - [使用権限 ARN] では、適切な使用権限を選択します。このリストには、自分に与えられたすべての使用権限が含まれます。

> **Tip**
>
> このフィールドをクリックして、使用権限名の入力を開始できます。MediaConnect は、入力したコンテンツと一致する名前の使用権限のみを含むようにリストをフィルタリングします。

7. ソースモニタリング設定で、有効にするモニタリング機能を選択します。

   a. サムネイル状態をオンにして、コンソールでプレビューできるソースサムネイルを生成します。

   b. コンテンツ品質分析の状態をオンにして、次のオーディオおよびビデオ品質の問題を監視します。

      i. (オプション) ブラックフレームをオンにして、ストリーム内のブラックビデオフレームの期間を検出します。

      ii. (オプション) フローズンフレームをオンにして、ストリーム内の変更されていないビデオフレームの期間を検出します。

      iii. (オプション) サイレントオーディオをオンにして、ストリーム内のオーディオサイレンス時間を検出します。

      iv. (オプション) 有効にするメトリクスごとに、10 ~ 60 秒の期間しきい値を設定します。デフォルト値は 30 秒です。

8. [フローの作成] を選択します。

次のステップ

フローを作成したら、以下のステップを実行してコンテンツの配信を開始します。

- MediaConnect フローがコンテンツを送信する場所を指定する出力を追加する
- 他のユーザーのユーザーがコンテンツを AWS アカウント サブスクライブできるようにする権限を付与します
- フローを開始してコンテンツ配信を開始する

その他のリソース

フローのソースモニタリングオプションの詳細については、このガイドの以下のページを参照してください。

- ソースビデオのサムネイルの表示
- でのコンテンツ品質分析によるモニタリング AWS Elemental MediaConnect

VPC ソースを使用するトランスポートストリームフローの作成

トランスポートストリームフローは、圧縮されたコンテンツを 1 つのストリームに多重化して転送します。

仮想プライベートクラウド (VPC) のソースを使用するフローを作成すると、コンテンツはパブリックインターネットを経由しません。これはセキュリティ上の理由だけでなく、信頼性の面でも役に立ちます。VPC を設定してから、その VPC へのインターフェイスを含むフローを作成します。代わりに、別の AWS アカウントに付与されたコンテンツ (使用権限のあるソース) または標準ソースの使用を許可する権限に基づいてフローを作成することもできます。

前提条件

開始する前に、次のステップを完了していることを確認してください。

VPC の構成

Amazon VPC で、VPC と関連するセキュリティグループを設定します。VPC の詳細については、「Amazon VPC ユーザーガイド」を参照してください。VPC インターフェイスと連携するようにセキュリティグループを設定する方法については、「セキュリティグループに関する考慮事項」を参照してください。

IAM セットアップ

IAM で、MediaConnect を信頼されたサービスとしてセットアップします。

暗号化設定 (必要な場合)

フローのソースで暗号化が必要な場合は、暗号化を設定します。

NDI® 設定 (NDI ユースケースのみ)

NDI 出力のドキュメントを確認して、開始する前にこの機能について理解しておくことをお勧めします。

フローに NDI 出力を追加する場合は、ネットワークに NDI 検出サーバーがプロビジョニングされた VPC が必要です。MediaConnect はこれらのサーバーに接続しますが、自動的には作成されません。

- AWS は、インストールと設定のベストプラクティスなど AWS CloudFormation、 を使用した複数のアベイラビリティーゾーンにわたる自動セットアップに関するガイダンスを提供します。手順については、「ブロードキャストワークフロー用の NDI 検出サーバーのセットアップ」を参照してください。
- 自己参照進入ルールと退出ルールを使用してセキュリティグループを設定することをお勧めします。その後、このセキュリティグループを、NDI サーバーが VPC 内で実行されている EC2 インスタンスにアタッチできます。このアプローチにより、VPC 内のコンポーネント間で必要なすべての NDI 通信が自動的に許可され、必要なすべてのネットワークトラフィックが許可されます。自己参照セキュリティグループルールの設定に関するガイダンスについては、「Amazon VPC ユーザーガイド」の「セキュリティグループの参照」を参照してください。

手順

VPC ソースを使用するトランスポートストリームフローを作成するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで [フローを作成] を選択します。
3. [詳細] セクションの [名前] で、フローの名前を指定します。この名前は、このフローの ARN の一部になります。

> **Note**
>
> MediaConnect では、同じ名前で複数のフローを作成できます。ただし、整理しやすいように、 AWS リージョン内では一意のフロー名を使用することをお勧めします。フローの作成後に、名前は変更できません。

4. [アベイラビリティーゾーン] では、任意を選択するか、VPC サブネットが存在するアベイラビリティーゾーンを選択します。これを [任意] のままにして、アベイラビリティーゾーンが正しく設定されていることをサービスに確認させることをお勧めします。
5. フローサイズで、ユースケースに合ったサイズを選択します。フローサイズの詳細については、「フローサイズと機能」を参照してください。

   中フローの場合：

   - ステップ 6 に直接進んでください。

   大きなフローの場合：

   - フローに NDI 出力が必要ない場合は、ステップ 6 に直接進んでください。
   - フローに NDI 出力を追加する場合は、次のように NDI 設定を行います。
     1. フロー NDI サポートを Enabled に設定します。
     2. (オプション) NDI マシン名を入力します。
        - この名前は、フローが作成する NDI ソースを識別するのに役立つプレフィックスとして使用されます。たとえば、 と入力すると**MACHINENAME**、NDI ソースは **MACHINENAME** として表示されます(`ProgramName`)。
        - 名前を入力しない場合、MediaConnect はプレフィックスとして一意の 12 文字の ID を生成します。この ID はフローの Amazon リソースネーム (ARN) から取得されるため、マシン名はフローリソースを参照します。

     > **Tip**
     >
     > NDI ソースを作成するフローが複数ある場合、慎重に命名することが特に重要です。たとえば、100 個の NDI ソースを持つ本番環境では、`STUDIO-A`、、などの明確でわかりやすいマシン名のプレフィックスが役立ちます`STUDIO-B`。`NEWSROOM`

3. 最大 3 つの NDI 検出サーバーを追加します。サーバーごとに、次の情報を指定します。
   - 既存の NDI インフラストラクチャのサーバー IP アドレスを入力します。
   - VPC インターフェイスアダプターを選択して、ネットワークアクセスを制御します。
   - (オプション) ポート番号を指定します。これを空白のままにすると、MediaConnect は NDI Discovery サーバーのデフォルトである TCP-5959 を使用します。

   > **Tip**
   >
   > 最大 3 つの検出サーバーを追加できます。複数の検出サーバーを持つことで信頼性が向上し、NDI ソースがネットワーク全体で検出可能になります。

6. [ソース] セクションで、[ソースタイプ] として [VPC ソース] を選択します。
7. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。
8. ソースがどのプロトコルを使用するかを決定します。

   > **Note**
   >
   > フェイルオーバー用の冗長ソースを指定する場合は、いずれかのソースを使用してフローを作成します。フローが作成されたら、ソースのフェイルオーバーを有効にするようにフローを更新し、2 つ目のソースをフローに追加します。MediaConnect は両方のソースをプライマリソースとして扱うため、最初にフローを作成するときにどちらを指定してもかまいません。

9. プロトコルに基づく具体的な説明については、以下のタブから 1 つ選択してください:

   RIST

   1. [プロトコル] には、[RIST] を選択します。
   2. [取り込みポート] には、フローが受信コンテンツをリッスンするポートを指定します。

      > **Note**
      >
      > RIST プロトコルでは、エラー修正のために 1 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから +1 されたポート

を予約します。例えば、出力にポート 4000 を指定すると、サービスにはポート 4000 と 4001 が割り当てられます。

3. [VPC インターフェイス名] には、ソースとして使用する VPC インターフェイスの名前を選択します。
4. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
5. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。1 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 2,000 ms を使用します。

RTP or RTP-FEC

1. [プロトコル] には、[RTP] または [RTP-FEC] を選択します。
2. [取り込みポート] には、フローが受信コンテンツをリッスンするポートを指定します。

> **Note**
>
> RTP-FEC プロトコルでは、エラー修正のために 2 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから+ 2 および +4 されたポートを予約します。例えば、出力にポート 4000 を指定すると、サービスにはポート 4000、4002、および 4004 が割り当てられます。

3. [VPC インターフェイス名] には、ソースとして使用する VPC インターフェイスの名前を選択します。
4. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。

SRT listener

1. [ソース] セクションで、[ソースタイプ] として [VPC ソース] を選択します。
2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウント以外のユーザーには表示されません。
3. [プロトコル] には、[SRT リスナー]を選択します。

4. [ソースの説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
5. [VPC インターフェイス名] には、ソースとして使用する VPC インターフェイスの名前を選択します。
6. [着信ポート] には、フローが着信コンテンツをリッスンするポートを指定します。
7. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
8. 最小レイテンシー には、サービスに保持させるバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。10 ~ 15,000 ミリ秒の値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 2,000 ms を使用します。

   SRT プロトコルは、接続の両側で最小レイテンシー設定を使用します。これら 2 つの値のうち大きい方を復旧レイテンシーとして使用します。送信ビットレートにリカバリレイテンシーを掛けた値が受信バッファよりも高い場合、バッファはオーバーフローし、ストリームは で失敗する可能性がありますBuffer Overflow Error。SRT レシーバー側では、レシーバーバッファは SRTO_RCVBUF 値によって設定されます。レシーバーバッファのサイズは、フロー制御ウィンドウサイズ (SRTO_FC) 値によって制限されます。MediaConnect 側では、レシーバーバッファは最大ビットレート値に最小レイテンシー値を乗算して計算されます。SRT バッファの詳細については、SRT 設定ガイドラインを参照してください。
9. ソースが暗号化されている場合は、[有効化] セクションで [有効化] を選択し、次の操作を行います。
   a. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
   b. シークレット ARN には、暗号化キーを保存するシークレットの作成時に が AWS Secrets Manager 割り当てた ARN を指定します。

SRT caller

1. [ソース] セクションで、[ソースタイプ] として [VPC ソース] を選択します。
2. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウント以外のユーザーには表示されません。
3. [プロトコル] には、[SRT コーラー] を選択します。

4. [ソースの説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
5. [VPC インターフェイス名] には、ソースとして使用する VPC インターフェイスの名前を選択します。
6. [ソースリスナーポート] には、フローがソースの取得に使用するポートを入力します。
7. [最大ビットレート] (オプション) には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
8. [最小遅延] には、サービスに保持させたいバッファ (遅延) の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。10 ~ 15,000 ミリ秒の値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。

   SRT プロトコルは、接続の両側で最小レイテンシー設定を使用します。これら 2 つの値のうち大きい方を復旧レイテンシーとして使用します。送信ビットレートに復旧レイテンシーを掛けた値が受信バッファよりも高い場合、バッファはオーバーフローし、ストリームは で失敗する可能性がありますBuffer Overflow Error。SRT レシーバー側では、レシーバーバッファは SRTO_RCVBUF 値によって設定されます。レシーバーバッファのサイズは、フロー制御ウィンドウサイズ (SRTO_FC) 値によって制限されます。MediaConnect 側では、レシーバーバッファは最大ビットレート値に最小レイテンシー値を乗算して計算されます。SRT バッファの詳細については、SRT 設定ガイドラインを参照してください。
9. [ストリーム ID] (オプション) には、ストリームの識別子を入力します。この識別子は、ストリームに関する情報を伝えるために使用できます。
10. ソースが暗号化されている場合は、[有効化] セクションで [有効化] を選択し、次の操作を行います。

    a. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。

    b. シークレット ARN には、暗号化キーを保存するシークレットの作成時に が AWS Secrets Manager 割り当てた ARN を指定します。

Zixi push

1. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウント以外のユーザーには表示されません。
2. [プロトコル] には [Zixi プッシュ] を選択します。

> **Note**
>
> MediaConnect は、作成時に Zixi プッシュ VPC ソースのインバウンドポートを割り当てます。2090 ~ 2099 のポート番号が自動的に割り当てられます。

3. [VPC インターフェイス名] には、ソースとして使用する VPC インターフェイスの名前を選択します。
4. [ストリーム ID] には、Zixi フィーダーに設定されているストリーム ID を指定します。

> **Important**
>
> このフィールドを空白のままにすると、サービスはソース名をストリーム ID として使用します。ストリーム ID は Zixi フィーダーに設定された値と一致する必要があるため、ソース名とまったく同じでない場合はストリーム ID を指定する必要があります。

5. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0 ~ 60,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。
6. ソースが暗号化されている場合は、[有効化] セクションで [有効化] を選択し、次の操作を行います。
   a. [復号化タイプ] には [静的キー] を選択します。
   b. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
   c. シークレット ARN には、暗号化キーを保存するシークレットの作成時に が AWS Secrets Manager 割り当てた ARN を指定します。
   d. [復号化アルゴリズム] では、ソースの暗号化に使用された暗号化のタイプを選択します。

10. フローに接続する VPC ごとに、次の手順を実行します。
    1. [VPC インターフェイス] セクションで、[VPC インターフェースを追加] を選択します。
    2. [名前] には、VPC インターフェイスの名前を指定します。VPC インターフェイスの名前は、フロー内で一意である必要があります。

3. ロール ARN では、MediaConnect を信頼できるサービスとして設定したときに作成したロールの Amazon リソースネーム (ARN) を指定します。
4. [VPC] では、使用する VPC の ID を選択します。

> **Note**
>
> 目的の VPC がリストに表示されない場合は、その VPC が Amazon Virtual Private Cloud で設定されており、その VPC を表示するための IAM 権限があることを確認してください。

5. [サブネット] では、MediaConnect が VPC 設定のセットアップに使用する VPC サブネットを選択します。少なくとも 1 つ選択する必要があり、必要な数だけ選択できます。
6. [セキュリティグループ] では、MediaConnect が VPC 設定のセットアップに使用する VPC セキュリティグループを指定します。少なくとも 1 つのセキュリティグループを選択する必要があります。

11. ソースモニタリング設定で、有効にするモニタリング機能を選択します。

    a. サムネイル状態をオンにして、コンソールでプレビューできるソースサムネイルを生成します。

    b. コンテンツ品質分析の状態をオンにして、次のオーディオおよびビデオ品質の問題を監視します。

        i. (オプション) ブラックフレームをオンにして、ストリーム内のブラックビデオフレームの期間を検出します。

        ii. (オプション) フローズンフレームをオンにして、ストリーム内の変更されていないビデオフレームの期間を検出します。

        iii. (オプション) サイレントオーディオをオンにして、ストリーム内のオーディオサイレンス時間を検出します。

        iv. (オプション) 有効にするメトリクスごとに、10 ~ 60 秒の期間しきい値を設定します。デフォルト値は 30 秒です。

12. ページの下部で、[今すぐ作成] を選択します。

次のステップ

フローを作成したら、以下のステップを実行してコンテンツの配信を開始します。

- MediaConnect フローがコンテンツを送信する場所を指定する出力を追加する
- 他のユーザーのユーザーがコンテンツを AWS アカウント サブスクライブできるようにする権限を付与します
- フローを開始してコンテンツ配信を開始する

その他のリソース

フローのソースモニタリングオプションの詳細については、このガイドの以下のページを参照してください。

- ソースビデオのサムネイルの表示
- でのコンテンツ品質分析によるモニタリング AWS Elemental MediaConnect

CDI フローの作成

CDI フローは、高品質の非圧縮コンテンツまたは軽く圧縮されたコンテンツを AWS クラウドとの間で転送します。JPEG XS を使用して軽く圧縮されたコンテンツを転送するように CDI フローを設定できます。コンテンツは、オーディオ、動画、または補助データ用に別々のメディアストリームに逆多重化されます。各 CDI フローでは、ソースに複数のメディアストリームを使用し、出力ごとに複数のメディアストリームを使用できます。MediaConnect は AWS Cloud Digital Interface（ AWS CDI) ネットワークテクノロジーを使用して、SMPTE 2110 のパート 22 トランスポート標準に準拠したコンテンツをトランスポートします。

CDI フローは、Amazon VPC を使用して設定した仮想プライベートクラウド (VPC) のソースのみをサポートします。VPC を設定してから、その VPC へのインターフェイスを含むフローを作成します。

MediaConnect は CDI フロー上の 2 つのソースをサポートしていません。ST 2110 JPEG XS ソースとの冗長性を確保するために、個々のメディアストリームに 2 つのインバウンド VPC インターフェイスを指定できます。CDI ソースとの冗長性を確保するために、2 番目のフローを作成します。

前提条件

この手順を開始する前に、以下のステップが完了していることを確認してください。

- 「CDI フローへのコントリビューション」に示されている推奨ワークフローを確認してください。
- Amazon VPC で、VPC と関連するセキュリティグループを設定します。VPC の詳細については、「Amazon VPC ユーザーガイド」を参照してください。VPC インターフェイスと連携するように

セキュリティグループを設定する方法については、「セキュリティグループに関する考慮事項」を参照してください。

- IAM で、MediaConnect を信頼されたサービスとしてセットアップします。

手順

AWS CDI フローを作成する (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで [フローを作成] を選択します。
3. [詳細] セクションの [名前] で、フローの名前を指定します。この名前は、このフローの ARN の一部になります。

   > **Note**
   >
   > MediaConnect では、同じ名前で複数のフローを作成できます。ただし、組織に役立つように、 AWS リージョン内で一意のフロー名を使用することをお勧めします。フローの作成後に、名前は変更できません。

4. [アベイラビリティーゾーン] では、VPC サブネットが存在するアベイラビリティーゾーンを選択します。
5. フローサイズで、ラージ 4x を選択します。
6. [ソース] セクションで、[ソースタイプ] として [VPC ソース] を選択します。
7. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。
8. [VPC インターフェイス] セクションに進んでください。
9. フローに接続する VPC ごとに、次の手順を実行します。

   1. [VPC インターフェイスを追加] を選択します。
   2. [名前] には、VPC インターフェイスの名前を指定します。VPC インターフェイスの名前は、フロー内で一意である必要があります。
   3. [タイプ] で、MediaConnect にこのインターフェイスで使用するネットワークアダプタのタイプを選択します。このインターフェイスを CDI ソースまたは出力に使用する場合は、タイプとして EFA を選択する必要があります。

4. ロール ARN では、MediaConnect を信頼できるサービスとして設定したときに作成したロールの Amazon リソースネーム (ARN) を指定します。
5. [VPC] では、使用する VPC の ID を選択します。

> **Note**
>
> 目的の VPC がリストに表示されない場合は、その VPC が Amazon Virtual Private Cloud で設定されており、その VPC を表示するための IAM 権限があることを確認してください。

6. [サブネット] では、MediaConnect が VPC 設定のセットアップに使用する VPC サブネットを選択します。少なくとも 1 つ選択する必要があり、必要な数だけ選択できます。
7. [セキュリティグループ] では、MediaConnect が VPC 設定のセットアップに使用する VPC セキュリティグループを指定します。少なくとも 1 つのセキュリティグループを選択する必要があります。

10. フローに追加するメディア ストリームごとに、次の手順を実行します。

1. [メディアストリーム] セクションで、[メディアストリームを追加] を選択します。
2. [名前] フィールドで、このメディアストリームをフロー内の他のメディアストリームと区別するのに役立つわかりやすい名前を指定します。
3. [説明] には、このメディアストリームの使用方法を覚えておくのに役立つ説明を指定します。
4. [ストリーム ID] には、メディアストリームの固有識別子を指定します。

   ソースまたはいずれかの出力が CDI プロトコルを使用している場合は、プロダクションシステムやプレイアウトシステムで想定される値を指定します。

   ソースとすべての出力が ST 2110 JPEG XS プロトコルを使用している場合は、フロー内の他のメディアストリームに固有の値を指定してください。
5. [詳細オプション] を選択すると、ストリームのタイプに基づいて追加オプションが表示されます。
6. ストリームのタイプに応じた詳細オプションの具体的な手順については、以下のタブのいずれかを選択してください。

   Audio

   a. [ストリームタイプ] には [オーディオ] を選択します。

b. [メディアクロックレート] には、ストリームのサンプルレートを指定します。この値は Hz 単位で測定されます。

c. [言語] には、オーディオの言語を指定します。この値は、レシーバーが認識できる形式である必要があります。

d. [チャンネルオーダー] では、オーディオチャンネルの形式を指定します。

e. [メディアストリームを追加] を選択します。

Video

a. [ストリームタイプ] には [動画] を選択します。

多くのフィールドでは、MediaConnect は推奨設定を表すデフォルト値を提供します。必要に応じてデフォルト値を変更してください。

b. [メディアクロックレート] はストリームのサンプルレートであり、90000 に設定されています。この値は Hz 単位で測定されます。

c. [ビデオ形式] には、ビデオの解像度を指定します。

d. [正確なフレームレート] には、ビデオのフレームレートを指定します。この値は 1 秒あたりのフレーム数で表す必要があります。

e. [色度測定] には、動画の色を表現するために使用された形式を指定します。

f. [スキャンモード] には、受信したビデオをスキャンするために使用された方法を指定します。

- 受信ビデオがインターレース (480i や 1080i など) の場合は、インターレースを選択します。
- 受信ビデオがプログレッシブ (720p や 1080p など) の場合は、プログレッシブを選択します。
- 受信ビデオが PSF (1080psf など) の場合は、プログレッシブセグメントフレームを選択します。

g. TCS には、ビデオで使用されていた転送特性システム (TCS) を指定します。

h. [範囲] には、ビデオのエンコード範囲を指定します。

i. PAR には、ビデオのピクセルアクセス率 (PAR) を指定します。

j. [メディアストリームを追加] を選択します。

Ancillary data

a. [ストリームタイプ] には、[補助データ] を選択します。

b. [メディアクロックレート] はストリームのサンプルレートであり、90000 に設定されています。この値は Hz 単位で測定されます。

c. [メディアストリームを追加] を選択します。

11. [ソース] セクションまで上にスクロールして戻ります。
12. ソースがどのプロトコルを使用するかを決定します。
13. プロトコルに基づく具体的な説明については、以下のタブから 1 つ選択してください:

CDI

1. [プロトコル] には [CDI] を選択します。
2. [説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
3. [インバウンドポート] には、フローが受信コンテンツをリッスンするポートを指定します。2077 と 2088 (これらのポートは他のプロトコル用に予約されています) を除いて、1024 ~ 65535 までの値を指定できます。
4. [VPC インターフェイス名] には、ソースとして使用する VPC インターフェースの名前を選択します。
5. ソースの一部として使用するメディアストリームごとに、次の手順を実行します。
   a. [メディアストリーム名] には、メディアストリームの名前を選択します。
   b. [エンコーディング名] では、デフォルト値をそのまま使用します。
      - 補助データストリームの場合、エンコーディング名は **smpte291** です。
      - オーディオストリームの場合、エンコーディング名は **pcm** です。
      - ビデオの場合、エンコーディング名は **raw** です。

ST 2110 JPEG XS

1. [プロトコル] には ST 2110 JPEG XS を選択します。
2. [説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
3. [最大同期バッファ] には、MediaConnect が受信ソース データを同期するために使用するバッファのサイズを指定します。この値はミリ秒 (ms) 単位で測定されます。
4. [VPC インターフェイス名 1] には、ソースとして使用する VPC インターフェイスを 1 つ選択します。
5. [VPC インターフェイス名 2] には、ソースとして使用する 2 番目の VPC インターフェイスを選択します。VPC インターフェイス 1 と 2 の間に優先順位はありません。
6. ソースの一部として使用するメディアストリームごとに、次の手順を実行します。

a. [メディアストリーム名] には、メディアストリームの名前を選択します。

b. [エンコーディング名] では、デフォルト値をそのまま使用します。

- 補助データストリームの場合、エンコーディング名は **smpte291** です。
- オーディオストリームの場合、エンコーディング名は **pcm** です。
- ビデオの場合、エンコーディング名は **jxsv** です。

c. [インバウンドポート] には、フローが受信コンテンツをリッスンするポートを指定します。2077 と 2088 (これらのポートは他のプロトコル用に予約されています) を除いて、1024 ~ 65535 までの値を指定できます。

14. ページの下部で、[今すぐ作成] を選択します。

> **Note**
>
> フローは自動的に開始しません。手動でフローを開始する必要があります。

15. 出力を追加して、MediaConnect がコンテンツを送信する場所を指定します。

AWS CDI フローを作成する (AWS CLI)

を使用してフロー AWS CLI を作成するには、 `create-flow` コマンドを使用する必要があります。フローの作成を簡単にするために、`create-flow` コマンドと `--cli-input-json` オプションを組み合わせて使用することをお勧めします。`--cli-input-json` オプションでは、新しいフローに必要な設定を含む JSON ファイルを作成する必要があります。この手順のステップ 1 では、この JSON ファイルを設定できる方法の例を示しています。`create-flow` コマンドと `--cli-input-json` オプションの詳細については、「AWS CLI コマンド リファレンスの作成フロー」を参照してください。

1. 作成するフローの詳細を含む JSON ファイルを作成します。

   次の例では、ファイルのコンテンツを示します。この例では、JPEG XS ソースを使用して、次の属性を持つ AWS CDI 出力を作成します。

   - 2 つの Amazon VPC インターフェイス、1 つの EFA (Elastic Fabric Adapter) と 1 つの ENA (Elastic Network Adapter)
   - 1 つのビデオストリーム、1 つのオーディオストリーム、および 1 つの補助データストリーム

```
{
```

```
    "Name": "AwardsShow",

    "MediaStreams": [
        {
            "Attributes": {
                "Fmtp": {
                    "Colorimetry": "BT709",
                    "ExactFramerate": "60000/1001",
                    "Par": "1:1",
                    "Range": "NARROW",
                    "ScanMode": "progressive",
                    "Tcs": "SDR"
                }
            },
            "ClockRate": 90000,
            "MediaStreamId": 0,
            "MediaStreamName": "video-stream",
            "MediaStreamType": "video",
            "VideoFormat": "1080p"
        },
        {
            "Attributes": {
                "Fmtp": {
                    "ChannelOrder": "SMPTE2110.(ST)"
                }
            },
            "ClockRate": 48000,
            "MediaStreamId": 1,
            "MediaStreamName": "audio-stream",
            "MediaStreamType": "audio"
        },
        {
            "ClockRate": 90000,
            "MediaStreamId": 2,
            "MediaStreamName": "anc-stream",
            "MediaStreamType": "ancillary-data"
        }
    ],

    "Outputs": [
        {
            "Name": "cdi-output",
            "Protocol": "cdi",
            "Description": "cdi-output to medialive",
```

```
            "Destination": "198.51.100.5",
            "MediaStreamOutputConfigurations": [
                {
                    "EncodingName": "raw",
                    "MediaStreamName": "video-stream"
                },
                {
                    "EncodingName": "pcm",
                    "MediaStreamName": "audio-stream"
                }
            ],
            "Port": 5000,
            "VpcInterfaceAttachment": {
                "VpcInterfaceName": "efa-name"
            }
        }
    ],

    "Source": {
        "Name": "jxs-input",
        "Protocol": "st2110-jpegxs",
        "Description": "jxs-input to cdi-output",
        "MaxSyncBuffer": 100,
        "MediaStreamSourceConfigurations": [
            {
                "EncodingName": "jxsv",
                "InputConfigurations": [
                    {
                        "InputPort": 5011,
                        "Interface": {
                            "Name": "efa-name"
                        }
                    },
                    {
                        "InputPort": 5011,
                        "Interface": {
                            "Name": "ena-name"
                        }
                    }
                ],
                "MediaStreamName": "video-stream"
            },
            {
                "EncodingName": "pcm",
```

```
                "InputConfigurations": [
                    {
                        "InputPort": 5001,
                        "Interface": {
                            "Name": "efa-name"
                        }
                    },
                    {
                        "InputPort": 5001,
                        "Interface": {
                            "Name": "ena-name"
                        }
                    }
                ],
                "MediaStreamName": "audio-stream"
            }
        ]
    },

    "VpcInterfaces": [
        {
            "Name": "efa-name",
            "NetworkInterfaceType": "efa",
            "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
            "SecurityGroupIds": [
                "sg-1234567890abcdef0"
            ],
            "SubnetId": "subnet-abcdef01234567890"
        },
        {
            "Name": "ena-name",
            "NetworkInterfaceType": "ena",
            "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
            "SecurityGroupIds": [
                "sg-1234567890abcdef0"
            ],
            "SubnetId": "subnet-abcdef01234567890"
        }
    ]
}
```

2. で AWS CLI、 `create-flow` コマンドを使用します。

```
aws mediaconnect create-flow --cli-input-json file://filename.json --
profile YourProfile
```

戻り値の例を以下に示します。

```
{
    "Flow": {
        "AvailabilityZone": "us-west-2a",
        "Description": "jxs-input to cdi-output",
        "EgressIp": "203.0.113.0",
        "Entitlements": [],
        "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
DwtfUlYOUVABAQNR-c94d84ce4215:AwardsShow",
        "MediaStreams": [
            {
                "Attributes": {
                    "Fmtp": {
                        "Colorimetry": "BT709",
                        "ExactFramerate": "60000/1001",
                        "Par": "1:1",
                        "Range": "NARROW",
                        "ScanMode": "progressive",
                        "Tcs": "SDR"
                    }
                },
                "ClockRate": 90000,
                "Fmt": 96,
                "MediaStreamId": 0,
                "MediaStreamName": "video-stream",
                "MediaStreamType": "video",
                "VideoFormat": "1080p"
            },
            {
                "Attributes": {
                    "Fmtp": {
                        "ChannelOrder": "SMPTE2110.(ST)"
                    }
                },
                "ClockRate": 48000,
                "Fmt": 97,
                "MediaStreamId": 1,
                "MediaStreamName": "audio-stream",
```

```
                "MediaStreamType": "audio"
            },
            {
                "ClockRate": 90000,
                "Fmt": 98,
                "MediaStreamId": 2,
                "MediaStreamName": "anc-stream",
                "MediaStreamType": "ancillary-data"
            }
        ],
        "Name": "AwardsShow",
        "Outputs": [
            {
                "Description": "cdi-output to medialive",
                "Destination": "198.51.100.5",
                "MediaStreamOutputConfigurations": [
                    {
                        "EncodingName": "raw",
                        "MediaStreamName": "video-stream"
                    },
                    {
                        "EncodingName": "pcm",
                        "MediaStreamName": "audio-stream"
                    }
                ],
                "Name": "cdi-output",
                "OutputArn": "arn:aws:mediaconnect:us-west-2:111122223333:output:1-
DwtfUlYOUVABAQNR-c94d84ce4215:cdi-output",
                "Port": 5000,
                "Transport": {
                    "Protocol": "cdi"
                },
                "VpcInterfaceAttachment": {
                    "VpcInterfaceName": "efa-name"
                }
            }
        ],
        "Source": {
            "Description": "jxs-input to cdi-output",
            "MediaStreamSourceConfigurations": [
                {
                    "EncodingName": "jxs-input",
                    "InputConfigurations": [
                        {
```

```
                            "InputIp": "203.0.113.1",
                            "InputPort": 5011,
                            "Interface": {
                                "Name": "efa-name"
                            }
                        },
                        {
                            "InputIp": "203.0.113.2",
                            "InputPort": 5011,
                            "Interface": {
                                "Name": "ena-name"
                            }
                        }
                    ],
                    "MediaStreamName": "video-stream"
                },
                {
                    "EncodingName": "pcm",
                    "InputConfigurations": [
                        {
                            "InputIp": "203.0.113.3",
                            "InputPort": 5001,
                            "Interface": {
                                "Name": "efa-name"
                            }
                        },
                        {
                            "InputIp": "203.0.113.4",
                            "InputPort": 5001,
                            "Interface": {
                                "Name": "ena-name"
                            }
                        }
                    ],
                    "MediaStreamName": "audio-stream"
                }
            ],
            "Name": "jxs-input",
            "SourceArn": "arn:aws:mediaconnect:us-west-2:111122223333:source:1-
DwtfUlYOUVABAQNR-c94d84ce4215:jxs-input",
            "Transport": {
                "MaxSyncBuffer": 100,
                "Protocol": "st2110-jpegxs"
            }
```

```
        },
        "Sources": [
            {
                "Description": "jxs-input to cdi-output",
                "MediaStreamSourceConfigurations": [
                    {
                        "EncodingName": "jxsv",
                        "InputConfigurations": [
                            {
                                "InputIp": "203.0.113.173",
                                "InputPort": 5011,
                                "Interface": {
                                    "Name": "efa-name"
                                }
                            },
                            {
                                "InputIp": "203.0.113.114",
                                "InputPort": 5011,
                                "Interface": {
                                    "Name": "ena-name"
                                }
                            }
                        ],
                        "MediaStreamName": "video-stream"
                    },
                    {
                        "EncodingName": "pcm",
                        "InputConfigurations": [
                            {
                                "InputIp": "203.0.113.173",
                                "InputPort": 5001,
                                "Interface": {
                                    "Name": "efa-name"
                                }
                            },
                            {
                                "InputIp": "203.0.113.114",
                                "InputPort": 5001,
                                "Interface": {
                                    "Name": "ena-name"
                                }
                            }
                        ],
                        "MediaStreamName": "audio-stream"
```

```
                    }
                ],
                "Name": "jxs-input",
                "SourceArn": "arn:aws:mediaconnect:us-west-2:111122223333:source:1-
DwtfUlYOUVABAQNR-c94d84ce4215:jxs-input",
                "Transport": {
                    "MaxSyncBuffer": 100,
                    "Protocol": "st2110-jpegxs"
                }
            }
        ],
        "Status": "STANDBY",
        "VpcInterfaces": [
            {
                "Name": "efa-name",
                "NetworkInterfaceIds": [
                    "eni-0ae6ca9ea6673a2a7"
                ],
                "NetworkInterfaceType": "efa",
                "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
                "SecurityGroupIds": [
                    "sg-1234567890abcdef0"
                ],
                "SubnetId": "subnet-abcdef01234567890"
            },
            {
                "Name": "ena-name",
                "NetworkInterfaceIds": [
                    "eni-0cbabcf978eeb00a2"
                ],
                "NetworkInterfaceType": "ena",
                "RoleArn": "arn:aws:iam::111122223333:role/MediaConnectAccessRole",
                "SecurityGroupIds": [
                    "sg-1234567890abcdef0"
                ],
                "SubnetId": "subnet-abcdef01234567890"
            }
        ]
    }
}
```

次のステップ

フローを作成したら、以下のステップを実行してコンテンツの配信を開始します。

- MediaConnect フローがコンテンツを送信する場所を指定する出力を追加する
- 他のユーザーのユーザーがコンテンツを AWS アカウント サブスクライブできるようにする権限を付与します
- フローを開始してコンテンツ配信を開始する

フローのリストの表示

特定の AWS リージョンの AWS Elemental MediaConnect フローのリストを表示できます。

フローのリスト (コンソール) を表示するには

- MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。

  コンテナ ページに、アカウントに関連付けられているすべてのコンテナが一覧表示されます。

フローのリスト (AWS CLI) を表示するには

- AWS CLI で、`list-flows` コマンドを使用します。

```
aws mediaconnect list-flows --profile PMprofile
```

戻り値の例を以下に示します。

```
{
  "Flows": [
    {
      "AvailabilityZone": "us-west-2a",
      "Description": "Temporary listed flow description",
      "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
      "Name": "BasketballGame",
      "SourceType": "OWNED",
      "Status": "STOPPING"
    },
    {
      "AvailabilityZone": "us-west-2d",
```

```
      "Description": "Temporary listed flow description",
      "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow",
      "Name": "AwardsShow",
      "SourceType": "OWNED",
      "Status": "STANDBY"
    }
  ]
}
```

フローの詳細の表示

ARN、アベイラビリティーゾーン、ステータス、ソース、使用権限、出力などのフローの詳細を表示できます。

フロー (コンソール) の詳細を表示するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、表示するフローの名前を選択します。

   そのフローの詳細ページが表示されます。このページは、以下のタブに分かれています。

   - ソース タブには、フローがソースに接続されているかどうかなど、このフローのソースに関する詳細が表示されます。
   - 出力 タブには、このフロー用に作成した各出力の詳細が表示されます。
   - 使用権限 タブには、このフローで付与した使用権限がすべて表示されます。
   - VPC インターフェース タブには、Amazon Virtual Private Cloud (Amazon VPC) サービスに基づく仮想プライベートクラウド (VPC) とのフローの接続のリストが表示されます。
   - メディアストリーム タブには、このフローで作成されたメディアストリームのリストが表示されます。各メディアストリームは、動画、オーディオ、補助データなど、動画のさまざまなコンポーネントを表します。
   - アラート タブには、このフローのアクティブなアラートのログが表示されます。

フロー (AWS CLI) の詳細を表示するには

- AWS CLI で、`describe-flow` コマンドを使用します。

```
aws mediaconnect describe-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow
```

戻り値の例を以下に示します。

```
{
    "Flow": {
        "EgressIp": "54.201.4.39",
        "AvailabilityZone": "us-east-1b",
        "Status": "ACTIVE",
        "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow",
        "Entitlements": [
            {
                "EntitlementArn": "arn:aws:mediaconnect:us-
east-1:111122223333:entitlement:1-AaBb11CcDd22EeFf-34DE5fG12AbC:MyEntitlement",
                "Description": "Assign to this account",
                "Name": "MyEntitlement",
                "Subscribers": [
                    "444455556666"
                ]
            }
        ],
        "Description": "NYC awards show",
        "Name": "AwardsShow",
        "Outputs": [
            {
                "Port": 2355,
                "Name": "NYC",
                "Transport": {
                    "SmoothingLatency": 0,
                    "Protocol": "rtp-fec"
                },
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYC",
                "Destination": "192.0.2.0"
            },
            {
                "Port": 3025,
                "Name": "LA",
                "Transport": {
                    "SmoothingLatency": 0,
```

```
                    "Protocol": "rtp-fec"
                },
                "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-987655dEF67hiJ89-c34de5fG678h:LA",
                "Destination": "192.0.2.0"
            }
        ],
        "Source": {
            "IngestIp": "54.201.4.39",
            "SourceArn": "arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:ShowSource",
            "Transport": {
                "MaxBitrate": 80000000,
                "Protocol": "rtp"
            },
            "IngestPort": 1069,
            "Description": "Saturday night show",
            "Name": "ShowSource",
            "WhitelistCidr": "10.24.34.0/23"
        }
    }
}
```

フローの開始

フローを作成したら、フローを開始する必要があります。フローはいつでも停止して再開することもできます。

フロー (コンソール) を開始するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、開始するフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [Start] (開始) を選択します。

フロー (AWS CLI) を開始するには

- AWS CLI で、`start-flow` コマンドを使用します。

```
aws mediaconnect start-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
profile PMprofile
```

戻り値の例を以下に示します。

```
{
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Status": "STARTING"
}
```

フローの停止

アクティブなフローを停止すると、AWS Elemental MediaConnect フローから直接、または使用権限を通じて出力にアクセスしている顧客は、そのフローをすぐに利用できなくなります。アクティブなフローを削除する場合は、フローを削除する前にフローを停止する必要があります。

フロー (コンソール) を停止するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、停止するフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [Stop] (停止) を選択します。

   DB インスタンスのステータスが スタンバイ に変更されます。フローはすぐに停止し、MediaConnect フローから直接出力にアクセスしている顧客や、使用権限を通じて出力にアクセスしている顧客には表示されなくなります。

フロー (AWS CLI) を停止するには

- AWS CLI で、`stop-flow` コマンドを使用します。

```
aws mediaconnect stop-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
profile PMprofile
```

戻り値の例を以下に示します。

```
{
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Status": "STOPPING"
}
```

フローの更新

フローが実行中であっても、フローのソース、使用権限、出力を変更できます。ただし、フローの名前、ARN、またはアベイラビリティーゾーンは変更できません。詳細については、次のトピックを参照してください。

- フロー上のタグの管理
- ソースの更新
- 出力の更新
- メディアストリームの更新
- 使用権限の更新
- VPC インターフェースをフローに追加する

フロー上のタグの管理

タグを使用することで、AWS Elemental MediaConnect のフロー、ソース、出力、および使用権限の請求先や組織を追跡しやすくなります。これらは AWS 請求書の整理に AWS Billing and Cost Management が提供するものと同じタグです。コスト配分でタグがどのように使用されているかについては、「AWS Billingユーザーガイド」の「コスト配分タグを使用したカスタム請求レポート」を参照してください。

フロー (コンソール) へタグを追加するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、タグを追加するフローの名前を選択します。

   そのフローの詳細ページが表示されます。

3. 詳細 セクションで、タグの管理 を選択します。
4. タグを管理 を選択し、タグを追加 を選択します。
5. 追加するタグごとに、以下が必要になります。

   a. キーと値を入力します。たとえば、キーを **sports**、値を **golf** にすることができます。

   b. [Add tag] (タグを追加) を選択します。
6. [Update] (更新) を選択します。

フロー (コンソール) のタグを編集するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、編集するタグを含むフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. 詳細 セクションで、タグの管理 を選択します。
4. [Manage tags] (タグの管理) を選択します。
5. 必要に応じて、タグを更新します。
6. [Update] (更新) を選択します。

フロー (コンソール) からタグを削除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、タグを追加するフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. 詳細 セクションで、タグの管理 を選択します。
4. [Manage tags] (タグの管理) を選択します。
5. 削除する各タグの横にある タグの削除 を選択します。
6. [Update] (更新) を選択します。

フローの削除

アクティブなフローを削除すると、AWS Elemental MediaConnect フローから直接、または使用権限を通じて出力にアクセスしている顧客は、そのフローをすぐに利用できなくなります。削除したフローは復元できません。

フローがアクティブな場合は、フローを停止してから削除する必要があります。

フロー (コンソール) を削除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、削除するフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. ステータス フィールドを確認して、フローが スタンバイ モードになっていることを確認します。
4. フローステータスが アクティブ の場合は、停止 を選択します。
5. [Delete] (削除) をクリックします。

   確認メッセージが表示されます。
6. フローの削除 を選択します。

   このフローは、MediaConnect フローから直接出力にアクセスしている顧客や、使用権限にアクセスしている顧客には表示されなくなります。フローが完全に削除されるまで、最大 5 分かかることがあります。

フロー (AWS CLI) を削除するには

- AWS CLI で、`delete-flow` コマンドを使用します。

```
aws mediaconnect delete-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
profile PMprofile
```

戻り値の例を以下に示します。

```
{
```

```
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Status": "DELETING"
}
```

AWS Elemental MediaConnect のソース

MediaConnect のソースは、次のようなライブビデオフィードを提供するものなら何でもかまいません。

- オンプレミスのエンコーダ
- 別の AWS Elemental MediaConnect フロー
- AWS Elemental MediaLive 出力
- プレイアウトシステム (クラウドベースまたはオンプレミス)

ソースに使用できるサポートされるプロトコルのリストについては、「プロトコル」を参照してください。

MediaConnect コンソールから、Amazon CloudWatch メトリクスを表示して、アクティブなフローのソースの状態を監視するできます。

トピック

- 既存のフローにソースを追加します
- フローのソースを更新します
- ソースフェイルオーバー
- ソースのタグの管理
- フローからソースを削除する
- ソースポート

既存のフローにソースを追加します

トランスポートストリームフローでは、フェイルオーバー用に 2 つ目のソースを追加できます。フロー上の両方のソースは、同じプロトコルを使用する必要があります。(ただし、一方のソースが RTP を使用し、もう一方のソースが RTP-FEC を使用する場合があります。) ソースフェイルオーバーについての詳細は、「ソースフェイルオーバー」を参照してください。

2 つ目のソースをフローに追加する方法は、使用するソースの種類によって異なります。

- 標準ソース : VPC ソースでも使用権限のあるソースでもない任意のソースからのコンテンツを使用します。

- VPC ソース：設定した VPC からのコンテンツを使用します。

MediaConnect は、使用権限のあるフローと CDI フローの 2 つのソースをサポートしていません。ST 2110 JPEG XS ソースとの冗長性を確保するために、個々のメディアストリームに 2 つのインバウンド VPC インターフェイスを指定できます。CDI ソースとの冗長性を確保するために、2 番目のフローを作成します。

MediaConnect コンソールから、Amazon CloudWatch メトリクスを表示して、アクティブなフローのソースの状態を監視するできます。

標準ソースを既存のフローに追加します

フェイルオーバー用に 2 つ目のソースを既存のフローに追加できます。フロー上の両方のソースは、同じプロトコルを使用する必要があります。（ただし、一方のソースが RTP を使用し、もう一方のソースが RTP-FEC を使用する場合があります。）ソースフェイルオーバーについての詳細は、「ソースフェイルオーバー」を参照してください。

既存のフローに標準ソースを追加するには（コンソール）

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フローページで、更新するフローの名前を選択します。
3. [ソース] タブを選択します。
4. ソースフェイルオーバー設定セクションで、編集を選択します。
5. [ソースフェイルオーバー設定の編集] ウィンドウで、[フェイルオーバー] が [アクティブ] に設定されていることを確認します。

   > **Note**
   >
   > 実行中のフローでフェイルオーバーを有効にすると、フロー出力が一時的に中断されることがあります。

6. [フェイルオーバーモード] のドロップダウンメニューで、ソースプロトコルで使用するモードを選択します。各プロトコルでサポートされているモードのリストについては、「ソースプロトコルのフェイルオーバーサポート」を参照してください。
7. [復旧期間] には、サービスに保持させたいバッファ（遅延）のサイズを指定します。バッファが大きいほど、ストリームの送信の遅延が長引きますが、エラー修正の余地が増えます。バッファが小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100–15000 ms の

間で値が選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 200 ms を使用します。

8. [更新] を選択します。
9. ソースセクションで編集を選択します。
10. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。
11. ソースタイプには、標準ソースを選択します。
12. ソースがどのプロトコルを使用するかを決定します。

> **Note**
>
> フロー上のすべてのソースは、同じプロトコルを使用する必要があります。ただし、一方のソースが RTP を使用し、もう一方のソースが RTP-FEC を使用する場合があります。

13. プロトコルに基づく具体的な説明については、以下のタブから 1 つ選択してください:

RIST

1. プロトコル には、RIST を選択します。
2. [着信ポート] には、フローが着信コンテンツをリッスンするポートを指定します。

> **Note**
>
> RIST プロトコルでは、エラー修正のために 1 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから +1 されたポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000 と 4001 が割り当てられます。

3. [許可リスト CIDR] では、ソースへのコンテンツの提供が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

4. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
5. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。1 ~ 15,000 ms の間で値が選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。

RTP or RTP-FEC

1. プロトコル には、RTP または RTP-FEC を選択します。
2. [着信ポート] には、フローが着信コンテンツをリッスンするポートを指定します。

> **Note**
>
> RTP-FEC プロトコルでは、エラー修正のために 2 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから+ 2 および +4 されたポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000、4002、および 4004 が割り当てられます。

3. [許可リスト CIDR] では、ソースへのコンテンツの提供が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

4. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。

SRT listener

1. プロトコルには、SRT リスナーを選択します。
2. [ソースの説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
3. [許可リスト CIDR ブロック] には、ソースへのコンテンツ提供を許可する IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

   > **Important**
   >
   > できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

4. [着信ポート] には、フローが着信コンテンツをリッスンするポートを指定します。
5. [ソースリスナーアドレス] には、MediaConnect が SRT 接続に使用するアドレスを入力します。アドレスは IP アドレスでもドメイン名でもかまいません。
6. [最大ビットレート] (オプション) には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
7. [最小遅延] には、サービスに保持させたいバッファ (遅延) の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。
8. ソースが暗号化されている場合は、[復号化] セクションで [有効化] を選択し、次の操作を行います。
   a. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
   b. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

SRT caller

1. プロトコル で [SRT コーラー] を選択します。
2. [ソースの説明] には、このソースの出所を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
3. [ソースリスナーアドレス] には、MediaConnect が SRT 接続に使用するアドレスを入力します。アドレスは IP アドレスでもドメイン名でもかまいません。
4. [ソースリスナーポート] には、MediaConnect が SRT 接続に使用するポートを入力します。
5. [最大ビットレート] (オプション) には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
6. [最小遅延] には、サービスに保持させたいバッファ (遅延) の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。
7. [ストリーム ID] (オプション) には、ストリームの識別子を入力します。この識別子は、ストリームに関する情報を伝えるために使用できます。
8. ソースが暗号化されている場合は、[復号化] セクションで [有効化] を選択し、次の操作を行います。
   a. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
   b. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

Zixi push

1. [プロトコル] には [Zixi プッシュ] を選択します。

   AWS Elemental MediaConnect は受信ポートの値を入力します。
2. [許可リスト CIDR] では、ソースへのコンテンツの提供が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

3. [ストリーム ID] には、Zixi フィーダーに設定されているストリーム ID を指定します。

> **Important**
>
> ストリーム ID は Zixi フィーダーに設定されている値と一致する必要があります。このフィールドを空白のままにすると、MediaConnect はソース名をストリーム ID として使用します。ストリーム ID がソース名と同じでない場合は、ストリーム ID を手動で入力する必要があります。

4. [最大遅延] には、サービスに保持させたいバッファ（遅延）のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0～60,000 ms の間で値が選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。
5. ソースが暗号化されている場合は、[復号化] セクションで [有効化] を選択し、次の操作を行います。
   a. [復号タイプ] には [スタティックキー] を選択します。
   b. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
   c. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。
   d. [復号化アルゴリズム] では、ソースの暗号化に使用された暗号化のタイプを選択します。

Zixi push for AWS Elemental Link UHD device

追加の Zixi プッシュソースを作成したら、MediaLive を使用して AWS Elemental Link デバイスを設定する必要があります。フローの作成後にプロセスを完了するには、次の MediaLive 設定手順「MediaLive ユーザーガイド」の「フロー内でのデバイスの使用」を参

照してください。これらの手順を完了するには、MediaConnect と MediaLive の両方にアクセスできることを確認してください。

> **Note**
>
> AWS Elemental Link UHD デバイス用 Zixi プッシュはフェイルオーバーモードのみをサポートします。マージモードはサポートされていません。

1. [プロトコル] には [Zixi プッシュ] を選択します。

   AWS Elemental MediaConnect は受信ポートの値を入力します。

2. [許可リスト CIDR] では、ソースへのコンテンツの提供が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

   > **Important**
   >
   > Link デバイスがインターネットへの接続に使用するパブリック IP アドレスの範囲がわかっている場合は、その CIDR ブロックを入力します。これは AWS Elemental Link デバイスの IP アドレスと同じではないことに注意してください。この情報を取得できない場合は、0.0.0.0/0 を使用して、考えられるすべての IP アドレスに対して開かれるように CIDR ブロックを設定できます。通常、インターネット全体 (0.0.0.0/0) に開かれる CIDR ブロックを割り当てることはベストプラクティスではありません。ただし、この方法を使用する必要がある場合、転送されるデータは AES-128 暗号化を使用して暗号化されます。

3. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0 ~ 60,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。最大遅延 の値は、AWS Elemental Link デバイスに設定されている 遅延 の値と一致する必要があります。リンクデバイスのレイテンシーの設定については、「AWS Elemental MediaLiveユーザーガイド」の「デバイスの設定」を参照してください。

4. 復号化 では、有効化 を選択し、次の操作を行います。

a. [復号タイプ] には [スタティックキー] を選択します。

b. [復号アルゴリズム] には [AES-128] を選択します。AWS Elemental Link には AES-128 が必要です。別のアルゴリズムは選択しないでください。

c. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。

d. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

14. [Save (保存)] を選択します。

VPC ソースを既存のフローに追加します

フェイルオーバー用に 2 つ目のソースを既存のトランスポートストリームフローに追加できます。フロー上のソースは両方ともバイナリで同一 (同じエンコーダーから取得) で、同じプロトコルを使用している必要があります。(ただし、一方のソースが RTP を使用し、もう一方のソースが RTP-FEC を使用する場合があります。) ソースフェイルオーバーについての詳細は、「ソースフェイルオーバー」を参照してください。

> **Important**
>
> この手順を開始する前に、以下のステップが完了していることを確認してください。
>
> - Amazon VPC で、VPC と関連するセキュリティグループを設定します。VPC の詳細については、Amazon VPC ユーザーガイドを参照してください。VPC インターフェイスと連携するようにセキュリティグループを設定する方法については、「セキュリティグループに関する考慮事項」を参照してください。
> - IAM で、MediaConnect を信頼されたサービスとしてセットアップします。
> - フローのソースで暗号化が必要な場合は、暗号化を設定してください。

MediaConnect は CDI フロー上の 2 つのソースをサポートしていません。ST 2110 JPEG XS ソースとの冗長性を確保するために、個々のメディアストリームに 2 つのインバウンド VPC インターフェイスを指定できます。CDI ソースとの冗長性を確保するために、2 番目のフローを作成します。

VPC ソースを既存のフローに追加するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フローページで、更新するフローの名前を選択します。

3. [ソース] タブを選択します。
4. ソースフェイルオーバー設定セクションで、編集を選択します。
5. [ソースフェイルオーバー設定の編集] ウィンドウで、[フェイルオーバー] が [有効] に設定されていることを確認します。

> **Note**
>
> 実行中のフローでフェイルオーバーを有効にすると、フロー出力が一時的に中断されることがあります。

6. [復旧期間] には、サービスに保持させたいバッファ（遅延）のサイズを指定します。バッファが大きいほど、ストリームの送信の遅延が長引きますが、エラー修正の余地が増えます。バッファが小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100–15000 ms の間で値が選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 200 ms を使用します。
7. [更新] を選択します。
8. ソースセクションで、ソースの追加を選択する。
9. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。
10. ソースタイプには、VPCソースを選択します。
11. ソースがどのプロトコルを使用するかを決定します。

> **Note**
>
> フロー上のすべてのソースは、同じプロトコルを使用する必要があります。ただし、一方のソースが RTP を使用し、もう一方のソースが RTP-FEC を使用する場合があります。

12. プロトコルに基づく具体的な説明については、以下のタブから 1 つ選択してください:

    RIST

    1. プロトコル には、RIST を選択します。
    2. [着信ポート] には、フローが着信コンテンツをリッスンするポートを指定します。

> **Note**
>
> RIST プロトコルでは、エラー修正のために 1 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから +1 されたポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000 と 4001 が割り当てられます。

3. [VPC インターフェース名] には、ソースとして使用する VPC インターフェースの名前を選択します。
4. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。
5. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。1 ~ 15,000 ms の間で値が選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。

RTP or RTP-FEC

1. [プロトコル] には、[RTP] または [RTP-FEC] を選択します。
2. [着信ポート] には、フローが着信コンテンツをリッスンするポートを指定します。

> **Note**
>
> RTP-FEC プロトコルでは、エラー修正のために 2 つの追加ポートが必要です。この要件に対応するために、MediaConnect は指定されたポートから+ 2 および +4 されたポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000、4002、および 4004 が割り当てられます。

3. [VPC インターフェース名] には、ソースとして使用する VPC インターフェースの名前を選択します。
4. [最大ビットレート] には、フローの最大期待ビットレート (ビット/秒) を指定します。実際のビットレートの 2 倍の値を指定することをお勧めします。

Zixi push

1. [プロトコル] には [Zixi プッシュ] を選択します。

   AWS Elemental MediaConnect は受信ポートの値を入力します。

2. [VPC インターフェース名] には、ソースとして使用する VPC インターフェースの名前を選択します。

3. [ストリーム ID] には、Zixi フィーダーに設定されているストリーム ID を指定します。

   > **Important**
   >
   > ストリーム ID は Zixi フィーダーに設定されている値と一致する必要があります。このフィールドを空白のままにすると、MediaConnect はソース名をストリーム ID として使用します。ストリーム ID がソース名と同じでない場合は、ストリーム ID を手動で入力する必要があります。

4. [最大遅延] には、サービスに保持させたいバッファ（遅延）のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0 ~ 60,000 ms の間で値が選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。

5. ソースが暗号化されている場合は、[復号化] セクションで [有効化] を選択し、次の操作を行います。

   a. [復号タイプ] には [スタティックキー] を選択します。

   b. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。

   c. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

   d. [復号化アルゴリズム] では、ソースの暗号化に使用された暗号化のタイプを選択します。

13. [Save (保存)] を選択します。

フローのソースを更新します

フローが現在実行中であっても、既存のフローのソースを更新できます。

既存のフローのソースを更新するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フローページで、更新するフローの名前を選択します。
3. [ソース] タブを選択します。
4. 更新するソースを選択します。
5. [更新] を選択します。
6. 適切な変更を行い、ソースの更新を選択します。

既存のフローのソースを更新するには (AWS CLI)

- AWS CLI で、update-flow-source コマンドを使用します。

```
aws mediaconnect update-flow-source --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow --source-
arn arn:aws:mediaconnect:us-east-1:111122223333:source:2-3aBC45dEF67hiJ89-
c34de5fG678h:AwardsShowSource --allowlist-cidr 10.24.34.0/24 --profile PMprofile
```

戻り値の例を以下に示します。

ソースフェイルオーバー

ソースフェイルオーバーは、トランスポートストリームフローに 2 つの冗長ソースを使用する設定です。この冗長性は、ビデオストリームの中断を、最小限に抑えるのに役立ちます。ソースフェイルオーバーを使用するには、フローに 2 つのソースを指定し、フェイルオーバーモードの 2 つのオプション (マージまたはフェールオーバー) のいずれかを選択します。

- マージモードでは、ソースストリームを 1 つのストリームに結合するので、単一ソースの損失から正常に回復できます。フェイルオーバーモードをマージに設定すると、MediaConnect に保持させたいバッファ (遅延) のサイズであるリカバリウィンドウを設定できます。復旧のウインドウが大きいほど、ストリームの送信の遅延が長引きますが、エラー修正の余地が増えます。復旧のウインドウが小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。この方法で使用するソースはバイナリで同一である必要があります。つまり、同じエンコーダーからのソースである必要があります。また、MediaConnect は 2 つのソースから同時にコンテンツを受信する必要があります。さらに、ソースが RTP プロトコルを使用する場合、シーケンス番号が揃った RTP ヘッダーが必要であり、SMPTE ST 2022-7 標準にも準拠している必要があります。

> **Note**
>
> SMPTE ST 2022-7 は、米国映画テレビ技術者協会 (SMPTE) グループによって開発された標準です。ST 2022-7 規格は、欠落したパケットを同一の冗長ストリームのパケットに置き換える方法を定義しています。このタイプのフェイルオーバーでは、MediaConnect が 2 つのストリームからパケットを回復するための時間を確保するために、ワークフローに小さな遅延バッファが必要です。

- フェイルオーバーモードでは、プライマリストリームとバックアップソースを切り替えることができます。この切り替えにより、より信頼性の高いストリームに簡単に移行できます。フェイルオーバーモードを フェイルオーバーに設定すると、ソースをプライマリソースとして指定できます。2 つ目のソースはバックアップとして機能します。プライマリソースを指定しない場合、MediaConnect は両方のソースを同じ優先順位で扱い、必要に応じて使用可能なソースに切り替えます。

MediaConnect は 2 つのフェイルオーバーモードを次のように使用します。

- マージモードでは、MediaConnect は両方のソースからのコンテンツを使用します。フローは、開始するソースの 1 つをランダムに選択します。ソースにパケットが欠落している場合、フローはもう一方のソースから欠落しているパケットを引き出します。たとえば、フローがソース A を使用しており、パケット 123 が欠落した場合、MediaConnect はソース B からパケット 123 を取り込み、ソース A を引き続き使用します。このモードでは、2 つのソースはバイナリで同一 / ST 2022-7 に準拠しています。
- フェイルオーバーモードでは、プライマリソースを指定しない場合、MediaConnect はソースの 1 つをランダムに使用してフローにコンテンツを提供します。MediaConnect がソースからデータを 500 ミリ秒間受信しない場合、フローはもう一方のソースに切り替わり、必要に応じてソース間の切り替えを続けることができます。プライマリソースを指定すると、MediaConnect はそのソースを使用してフローにコンテンツを提供します。プライマリソースが 500 ミリ秒間データを送信しない場合、フローはもう一方のソースに切り替わり、データが戻るとすぐにプライマリソースに切り替わります。

> **Note**
>
> MediaConnect は CDI フローまたはエンタイトルメントフローでのソースフェイルオーバーをサポートしていません。CDI フローによる冗長性の作成について詳しくは、「CDI フロー

の作成」を参照してください。また、Zixi プルプロトコルまたは富士通 QoS プロトコルを使用している場合は、フェイルオーバー用の既存のフローに 2 つ目のソースを追加することはできません。

ソースプロトコルのフェイルオーバーサポート

次のテーブルは、どのソースプロトコルがフェイルオーバーをサポートしているかをまとめたものです。

プロトコル	このプロトコルはソースフェイルオーバーをサポートしていますか？	ソースはいくつ追加できますか？	サポートされるフェイルオーバーモード
RIST	Yes	2	マージまたはフェイルオーバー
RTP	Yes	2	マージまたはフェイルオーバー
RTP-FEC	Yes	2	マージまたはフェイルオーバー
SRT リスナー	Yes	2	フェイルオーバーのみ
SRT コーラー	Yes	2	フェイルオーバーのみ
Zixi プル	No	なし：Zixi プルはソースとして使用できません。	ソースフェイルオーバーはサポートされていません。
Zixi プッシュ	Yes	2	マージまたはフェイルオーバー
AWS Elemental Link UHD 用 Zixi プッシュ	Yes	2	フェイルオーバーのみ

プロトコル	このプロトコルはソースフェイルオーバーをサポートしていますか？	ソースはいくつ追加できますか？	サポートされるフェイルオーバーモード
Fujitsu-QoS	No	1	ソースフェイルオーバーはサポートされていません。
CDI	No	1	ソースフェイルオーバーはサポートされていません。
ST 2110 JPEG XS	No	1	ソースフェイルオーバーはサポートされていません。
エンタイトルメントフロー	No	1	ソースフェイルオーバーはサポートされていません。

ソースのタグの管理

タグを使用することで、AWS Elemental MediaConnect のフロー、ソース、出力、および使用権限の請求先や組織を追跡しやすくなります。これらは AWS 請求書の整理に AWS Billing and Cost Management が提供するものと同じタグです。コスト配分でタグがどのように使用されているかについては、「AWS Billingユーザーガイド」の「コスト配分タグを使用したカスタム請求レポート」を参照してください。

ソース(コンソール) へタグを追加するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを追加するソースに関連するフローの名前を選択します。
3. [ソース] タブを選択します。

   そのソースの出力リストが表示されます。
4. タグを追加するソースを選択します。

5. [Manage tags] (タグの管理) を選択します。
6. [タグを管理]をもう一度選択し、[新しいタグを追加]を選択します。
7. 追加するタグごとに、以下が必要になります。

   a. キーと値を入力します。たとえば、キーを **sports**、値を **golf** にすることができます。

   b. [Add tag] (タグを追加) を選択します。
8. [更新] を選択します。

ソース (コンソール) のタグを編集するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを編集するソースに関連するフローの名前を選択します。
3. [ソース] タブを選択します。

   そのソースの出力リストが表示されます。
4. タグを編集するソースを選択します。
5. [Manage tags] (タグの管理) を選択します。
6. もう一度 [タグの管理] を選択します。
7. 必要に応じて、タグを更新します。
8. [更新] を選択します。

ソースからタグを削除するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを削除するソースに関連するフローの名前を選択します。
3. [ソース] タブを選択します。

   そのソースの出力リストが表示されます。
4. タグを削除するソースを選択します。
5. [Manage tags] (タグの管理) を選択します。
6. もう一度 [タグの管理] を選択します。
7. 削除するタグの横にある [タグの削除] を選択します。
8. [更新] を選択します。

フローからソースを削除する

フローに複数のソースがある場合、フローが現在実行中であってもソースの 1 つを削除できます。

フローからソースを削除するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フローページで、フローの名前を選択します。
3. [ソース] タブを選択します。
4. 削除するソースを選択します。
5. [Remove] (削除) を選択します。

ソースポート

フロー上の各ソースは異なるポートを使用する必要があります (例外については注記を参照してください)。一部のプロトコルでは、エラー修正のために追加のポートが必要です。これらのプロトコルを使用するソースの場合、AWS Elemental MediaConnect は必要な追加ポートを自動的に予約します。次の表は、サービスが予約する追加ポート (ある場合) の一覧です。

> **Note**
>
> Zixi プロトコルを使用するソースのポート要件には例外があります。標準 Zixi ソースでは、すべてのソースがポート 2088 を使用します。VPC Zixi ソースの場合、ソースは 2090〜2099 のインバウンドポート範囲を使用します。VPC Zixi ソースポートは、ソースの作成時に MediaConnect によって割り当てられます。

プロトコル	必要なポート	必須ポート
CDI	ポート	指定するポート。ソースに必要なポートはこれだけです。
RIST	ポートとポート +1	指定したポートと 1 つの追加ポート。MediaConnect は、指定したポートから +1 されたポートを自動的に予約します。

プロトコル	必要なポート	必須ポート
		たとえば、出力にポート 3000 を指定すると、サービスはポート 3001 も予約します。
RTP	ポート	指定するポート。出力に必要なポートはこれだけです。
RTP-FEC	ポート、ポート +2、ポート +4	指定したポートと 2 つの追加ポート。MediaConnect は、指定したポートから +2 と +4 のポートを自動的に予約します。 たとえば、出力にポート 2000 を指定すると、サービスはエラー修正用にポート 2002 と 2004 も予約します。
SRT リスナー	ポート	指定するポート。ソースに必要なポートはこれだけです。
SRT コーラー	ポート	指定するポート。ソースに必要なポートはこれだけです。
Fujitsu-QoS	ポートとポート +1	指定したポートと 1 つの追加ポート。MediaConnect は、指定したポートから +1 されたポートを自動的に予約します。
ST 2110 JPEG XS	ポート	指定するポート。ソースに必要なポートはこれだけです。

プロトコル	必要なポート	必須ポート
Zixi プッシュ	ポート	標準ソースの場合：MediaConnect は自動的にポート 2088 を使用します。 VPC ソースの場合：MediaConnect は、ソースの作成時に 2090 ~ 2099 の範囲のポートを自動的に割り当てます。

MediaConnect の出力

出力とは、MediaConnect にフローのコンテンツを送信するさまざまな宛先です。フローがアクティブな場合でも、いつでも出力を追加および削除できます。これらの出力は、指定した IP アドレスに送信されます。このオプションは、コンテンツをオンプレミスのエンコーダーに送信する場合に便利です。

トランスポートストリームフローの場合、別の AWS アカウント (サブスクライバーアカウント) とコンテンツを共有する権限を付与できます。サブスクライバーがコンテンツをソースとして使用してフローを作成すると、AWS Elemental MediaConnect はフローに関する出力を生成します。

> **Note**
>
> サブスクライバーがその使用権限に基づいてフローを作成した後で使用権限を無効にしても、関連する出力はフローに残ります。この出力は引き続き出力の最大数にカウントされます。使用権限に関連付けられている出力を削除するには、使用権限を取り消します。

トピック

- 出力をフローに追加する
- フローの出力リストの表示
- フローの出力の更新
- 出力のタグの管理
- フローからの出力の削除
- HTTP 送信先
- 出力の IP アドレスの決定

出力をフローに追加する

トランスポートストリームフローには、最大 50 個の出力を追加できます。ただし、最適なパフォーマンスを得るには、「ベストプラクティス」に記載されているガイダンスに従ってください。すべての出力には、名前、プロトコル、IP アドレス、ポートが必要です。

> **Note**
>
> 出力の使用権限を設定する場合、出力を作成しないでください。代わりに、使用権限を付与します。サブスクライバーがコンテンツをソースとして使用してフローを作成すると、サービスはフローに出力を作成します。

フローに出力を追加するときに使用する方法は、追加する出力のタイプによって異なります。

- 標準出力 (トランスポートストリームフロー) — Amazon Virtual Private Cloud を使用して設定した仮想プライベートクラウド (VPC) 以外の宛先に圧縮コンテンツを送信します。
- VPC 出力 (トランスポートストリームフロー) — Amazon Virtual Private Cloud を使用して設定した VPC に圧縮コンテンツを送信します。
- VPC 出力 (CDI フロー) — Amazon Virtual Private Cloud を使用して設定した VPC に圧縮されていないコンテンツを送信します。

標準出力をフローに追加する

トランスポートストリームフローには、最大 50 個の出力を追加できます。ただし、最適なパフォーマンスを得るには、「ベストプラクティス」に記載されているガイダンスに従ってください。標準出力は、Amazon Virtual Private Cloud (VPC) を使用して作成した仮想プライベートクラウド (VPC) に含まれないすべての宛先に送信されます。

> **Note**
>
> CDI フローは標準出力をサポートしていません。

標準出力をフロー (コンソール) に追加するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、出力を追加するフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [出力] タブを選択します。
4. [出力の追加] を選択します。

5. [名前] に、出力の名前を指定します。この値は、AWS Elemental MediaConnect コンソールにのみ表示される識別子であり、エンドユーザーには表示されません。
6. [出力タイプ] には 標準出力を選択します。
7. [説明] には、この出力先を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
8. 出力に使用するプロトコルを決定します。
9. 使用するプロトコルに基づいた具体的な手順については、以下のタブから 1 つ選択してください。

RIST

1. プロトコル には、RIST を選択します。
2. [IP アドレス] には、出力を送信する IP アドレスを選択します。
3. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。

> **Note**
>
> RIST プロトコルでは、エラー修正のために 1 つの追加ポートが必要です。この要件に対応するため、AWS Elemental MediaConnect は指定されたポート番号 +1 のポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000 と 4001 が割り当てられます。

4. [平滑化レイテンシー] には、出力の平滑化に使用する追加遅延を指定します。スムージングを無効にするには、値を 0 ms に指定することをお勧めします。ただし、レシーバーがストリームを適切に処理できない場合は、100 ~ 1,000 ms の値を指定してください。このようにして、AWS Elemental MediaConnect はフローソースからのジッターの修正を試みます。このフィールドを空白のままにすると、サービスはデフォルト値の 0 ms を使用します。

RTP or RTP-FEC

1. [プロトコル] には、RTP または RTP-FEC を選択します。
2. [IP アドレス] には、出力を送信する IP アドレスを選択します。
3. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。

> **Note**
>
> RTP-FEC プロトコルでは、エラー修正のために 2 つの追加ポートが必要です。この要件に対応するために、AWS Elemental MediaConnect は指定されたポート番号+ 2 および +4 のポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000、4002、および 4004 が割り当てられます。

4. [平滑化レイテンシー] には、出力の平滑化に使用する追加遅延を指定します。スムージングを無効にするには、値を 0 ms に指定することをお勧めします。ただし、レシーバーがストリームを適切に処理できない場合は、100 ~ 1,000 ms の値を指定してください。このようにして、AWS Elemental MediaConnect はフローソースからのジッターの修正を試みます。このフィールドを空白のままにすると、サービスはデフォルト値の 0 ms を使用します。

SRT listener

1. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。
2. プロトコル には、SRT リスナーを選択します。
3. [最小遅延] には、サービスに保持させたいバッファ（遅延）の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。
4. [CIDR 許可リスト] では、出力からのコンテンツの表示が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

5. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
6. この出力に送信されるビデオを暗号化する場合は、次の操作を行います。
   a. [暗号化] セクションで有効化を選択します。
   b. [暗号化タイプ] は選択できません。このプロトコルで使用できる暗号化は srt-パスワードだけです。
   c. [ロール ARN] には、暗号化を設定するときに作成したロールの ARN を指定します。
   d. [シークレット ARN] には、SRT パスワードを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

SRT caller

1. [プロトコル] で SRT 発信者を選択します。
2. [最小遅延] には、サービスに保持させたいバッファ（遅延）の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。
3. [宛先 IP アドレス] には、出力先の IP アドレスまたはドメインを入力します。
4. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
5. この出力に送信されるビデオを暗号化する場合は、次の操作を行います。
   a. [暗号化] セクションで有効化を選択します。
   b. [暗号化タイプ] は選択できません。このプロトコルで使用できる暗号化は SRT-パスワードだけです。
   c. [ロール ARN] には、暗号化を設定するときに作成したロールの ARN を指定します。
   d. [シークレット ARN] には、SRT パスワードを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

Fujitsu-QoS

1. [プロトコル] には、Fujitsu-QoS を選択します。

2. [ポート] には、レシーバーと制御パケットを交換するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
3. [CIDR 許可リスト] では、出力からのコンテンツの表示が許可される IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

> **Important**
>
> できるだけ正確な CIDR ブロックを指定してください。フローにコンテンツを提供する IP アドレスのみを含めてください。指定した CIDR ブロックが広すぎると、外部の第三者がフローにコンテンツを送信する可能性があります。

Zixi pull

1. [プロトコル] には Zixi プルを選択します。
2. [ストリーム ID] には、Zixi レシーバーに入力を追加したときに設定したストリーム値を入力します。Zixi レシーバーでは、この値は [ストリームパラメーター] セクションにあります。

> **Important**
>
> このフィールドを空白のままにすると、サービスは出力名をストリーム ID として使用します。ストリーム ID は Zixi レシーバーに設定されている値と一致する必要があるため、ストリーム ID が出力名とまったく同じでない場合はストリーム ID を指定する必要があります。

3. [リモート ID] には、Zixi レシーバーに割り当てられている ID 値を入力します。Zixi レシーバーでは、この値は [一般] 設定メニューにあり、ID というラベルが付いています。ID 値は Zixi レシーバーの [ステータス] ページにも表示されます。
4. [最大遅延] には、サービスに保持させたいバッファ (遅延) のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0 ~ 60,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはレシーバーで設定されている遅延を使用します。

5. [CIDR 許可リスト] の場合、ソースからのコンテンツの取得を許可する IP アドレスの範囲を指定します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.24.34.0/23 など) としてフォーマットします。CIDR 表記の詳細については、RFC 4632 を参照してください。

   > **Tip**
   >
   > 追加の CIDR ブロックを指定するには、[追加] を選択します。CIDR ブロックは最大 3 つまで指定できます。

6. この出力に送信されるビデオを暗号化する場合は、次の操作を行います。
   a. [暗号化] セクションで有効化を選択します。
   b. [暗号化タイプ] には、静的キーを選択します。
   c. [ロール ARN] には、暗号化を設定するときに作成したロールの ARN を指定します。
   d. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。
   e. [暗号化アルゴリズム] には、ソースの暗号化に使用する暗号化の種類を選択します。

Zixi push

1. [プロトコル] には、Zixi プッシュを選択します。
2. [IP アドレス] には、出力を送信する IP アドレスを選択します。
3. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
4. [ストリーム ID] には、Zixi レシーバーに設定されているストリーム ID を入力します。

   > **Important**
   >
   > このフィールドを空白のままにすると、サービスは出力名をストリーム ID として使用します。ストリーム ID は Zixi レシーバーに設定されている値と一致する必要があるため、ストリーム ID が出力名とまったく同じでない場合はストリーム ID を指定する必要があります。

5. [最大遅延] には、サービスに保持させたいバッファ（遅延）のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も

少なくなります。0 ~ 60,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。

6. この出力に送信されるビデオを暗号化する場合は、次の操作を行います。

   a. [暗号化] セクションで有効化を選択します。

   b. [暗号化タイプ] には、静的キーを選択します。

   c. [ロール ARN] には、暗号化を設定するときに作成したロールの ARN を指定します。

   d. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

   e. [暗号化アルゴリズム] には、ソースの暗号化に使用する暗号化の種類を選択します。

10. [出力の追加] を選択します。

出力をフロー (AWS CLI) に追加するには

1. フローに追加する出力の詳細を含む JSON ファイルを作成します。

   次の例では、ファイルのコンテンツを示します。

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "Outputs": [
        {
            "Description": "RTP-FEC Output",
            "Destination": "192.0.2.12",
            "Name": "RTPOutput",
            "Port": 5020,
            "Protocol": "rtp-fec",
            "SmoothingLatency": 100
        }
    ]
}
```

2. AWS CLI で、add-flow-output コマンドを使用します。

```
aws mediaconnect add-flow-outputs --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --cli-
input-json file://addFlowOutput.txt --region us-west-2
```

戻り値の例を以下に示します。

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "Outputs": [
        {
            "Name": "RTPOutput",
            "Port": 5020,
            "Transport": {
                "SmoothingLatency": 100,
                "Protocol": "rtp-fec"
            },
            "Destination": "192.0.2.12",
            "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:RTPOutput",
            "Description": "RTP-FEC Output"
        }
    ]
}
```

VPC 出力をフローに追加する

VPC 出力は、Amazon Virtual Private Cloud を使用して作成した仮想プライベートクラウド (VPC) に送信されます。

トランスポートストリームフローの場合、フローがアクティブであっても出力は最大 50 個まで追加できます。CDI フローでは、フローがスタンバイモードの場合にのみ、出力 (最大 10 個) を追加できます。最適なパフォーマンスを得るには、「ベストプラクティス」に記載されているガイダンスに従ってください。

VPC 出力をフロー (コンソール) に追加するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、出力を追加するフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [出力] タブを選択します。
4. [出力の追加] を選択します。

5. [名前] に、出力の名前を指定します。この値は、AWS Elemental MediaConnect コンソールにのみ表示される識別子であり、エンドユーザーには表示されません。
6. [出力タイプ] には、VPC 出力を選択します。
7. [プロトコル] には、適切なプロトコルを選択します。
8. [説明] には、この出力先を後で確認できるように説明を入力します。これは、会社名または設定に関するメモである可能性があります。
9. 出力に使用するプロトコルを決定します。プロトコルのオプションはフロータイプによって異なります。

   - トランスポートストリームフローの場合、プロトコルのオプションには RTP、RTP-FEC、RIST、SRT、および Zixi があります。
   - CDI フローの場合、プロトコルのオプションには CDI および ST 2110 JPEG XS があります。

10. 使用するプロトコルに基づいた具体的な手順については、以下のタブから 1 つ選択してください。

    RIST

    1. [プロトコル] には、RIST を選択します。
    2. [IP アドレス] には、出力を送信する IP アドレスを選択します。
    3. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。

       > **Note**
       >
       > RIST プロトコルでは、エラー修正のために 1 つの追加ポートが必要です。この要件に対応するため、AWS Elemental MediaConnect は指定されたポート番号 +1 のポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000 と 4001 が割り当てられます。

    4. [平滑化レイテンシー] には、出力の平滑化に使用する追加遅延を指定します。スムージングを無効にするには、値を 0 ms に指定することをお勧めします。ただし、レシーバーがストリームを適切に処理できない場合は、100 ~ 1,000 ms の値を指定してください。このようにして、AWS Elemental MediaConnect はフローソースからのジッターの修正を試みます。このフィールドを空白のままにすると、サービスはデフォルト値の 0 ms を使用します。

5. [VPC への出力] では、出力送信先の VPC インターフェイスの名前を選択します。

RTP or RTP-FEC

1. [プロトコル] には、RTP または RTP-FEC を選択します。

> **Note**
>
> RTP 出力と RTP-FEC 出力は SMPTE 2022-7 規格に準拠しています。ダウンストリームにあるレシーバーが2022-7 のソースマージをサポートしている場合、RTP 出力と RTP-FEC 出力は互換性があります。

2. [IP アドレス] には、出力を送信する IP アドレスを選択します。
3. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。

> **Note**
>
> RTP-FEC プロトコルでは、エラー修正のために 2 つの追加ポートが必要です。この要件に対応するために、AWS Elemental MediaConnect は指定されたポート番号+ 2 および +4 のポートを予約します。たとえば、出力にポート 4000 を指定すると、サービスにはポート 4000、4002、および 4004 が割り当てられます。

4. [平滑化レイテンシー] には、出力の平滑化に使用する追加遅延を指定します。スムージングを無効にするには、値を 0 ms に指定することをお勧めします。ただし、レシーバーがストリームを適切に処理できない場合は、100 ~ 1,000 ms の値を指定してください。このようにして、AWS Elemental MediaConnect はフローソースからのジッターの修正を試みます。このフィールドを空白のままにすると、サービスはデフォルト値の 0 ms を使用します。
5. [VPC への出力] では、出力送信先の VPC インターフェイスの名前を選択します。

SRT listener

1. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。
2. [出力タイプ] には、VPC 出力を選択します。

3. [プロトコル] には、SRT リスナーを選択します。
4. [説明] には、ある出力を別の出力と区別するのに役立つ説明を入力します。これは、会社名または設定に関するメモである可能性があります。
5. [最小遅延] には、サービスに保持させたいバッファ（遅延）の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。
6. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
7. [VPC への出力] では、出力送信先の VPC インターフェイスの名前を選択します。
8. この出力に送信されるビデオを暗号化する場合は、次の操作を行います。
   a. [暗号化] セクションで有効化を選択します。
   b. [ロール ARN] には、暗号化を設定するときに作成したロールの ARN を指定します。
   c. [シークレット ARN] には、SRT パスワードを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

SRT caller

1. [名前] には、ソースの名前を指定します。この値は、MediaConnect コンソールでのみ表示される識別子です。現在の AWS アカウントの外部には表示されません。
2. [出力タイプ] には、VPC 出力を選択します。
3. [プロトコル] には、SRT コーラーを選択します。
4. [説明] には、ある出力を別の出力と区別するのに役立つ説明を入力します。これは、会社名または設定に関するメモである可能性があります。
5. [最小遅延] には、サービスに保持させたいバッファ（遅延）の最小サイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。100 ~ 15,000 ms までの値を選択できます。このフィールドを空白のままにすると、MediaConnect はデフォルト値の 2,000 ms を使用します。
6. [宛先 IP アドレス] には、出力先の IP アドレスまたはドメインを入力します。
7. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。

8. [VPC への出力] では、出力送信先の VPC インターフェイスの名前を選択します。
9. この出力に送信されるビデオを暗号化する場合は、次の操作を行います。
   a. [暗号化] セクションで有効化を選択します。
   b. [暗号化タイプ] は選択できません。このプロトコルで使用できる暗号化は SRT-パスワードだけです。
   c. [ロール ARN] には、暗号化を設定するときに作成したロールの ARN を指定します。
   d. [シークレット ARN] には、SRT パスワードを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

Zixi push

1. [プロトコル] には、Zixi プッシュを選択します。
2. [IP アドレス] には、出力を送信する IP アドレスを選択します。
3. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
4. [ストリーム ID] には、Zixi レシーバーに設定されているストリーム ID を入力します。

> **Important**
>
> このフィールドを空白のままにすると、サービスは出力名をストリーム ID として使用します。ストリーム ID は Zixi レシーバーに設定されている値と一致する必要があるため、ストリーム ID が出力名とまったく同じでない場合はストリーム ID を指定する必要があります。

5. [最大遅延] には、サービスに保持させたいバッファ（遅延）のサイズを指定します。レイテンシーの値が大きいほど、ストリーム送信の遅延が長引きますが、エラー修正の余地が増えます。レイテンシーの値が小さいほど、遅延は短くなりますが、エラー修正の余地も少なくなります。0 ~ 60,000 ms までの値を選択できます。このフィールドを空白のままにすると、サービスはデフォルト値の 6,000 ms を使用します。
6. [VPC への出力] では、出力送信先の VPC インターフェイスの名前を選択します。
7. この出力に送信されるビデオを暗号化する場合は、次の操作を行います。
   a. [暗号化] セクションで有効化を選択します。
   b. [暗号化タイプ] には、静的キーを選択します。
   c. [ロール ARN] には、暗号化を設定するときに作成したロールの ARN を指定します。

d. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。

e. [暗号化アルゴリズム] には、ソースの暗号化に使用する暗号化の種類を選択します。

Fujitsu-QoS

1. [プロトコル] には、Fujitsu-QoS を選択します。
2. [ポート] には、レシーバーと制御パケットを交換するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
3. [VPC への出力] では、出力送信先の VPC インターフェイスの名前を選択します。

CDI

1. プロトコル には CDI を選択します。
2. [IP アドレス] には、出力を送信する IP アドレスを選択します。
3. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
4. [VPC インターフェイス] では、出力の送信先となる VPC インターフェイスの名前を選択します。
5. 出力の一部として送信するメディアストリームごとに、次の操作を行います。

   a. [メディアストリーム名] には、メディアストリームの名前を選択します。フロー上のソースが使用するメディアストリームのみを追加できます。

   b. [エンコーディング名] には、メディアストリームのタイプに基づいて事前に選択されているデフォルト値を確認します。

   c. [FMT には、メディアストリームのフォーマットタイプ番号 (RTP ペイロードタイプと呼ばれることもあります) を指定します。この値は、レシーバーが認識できる形式である必要があります。

ST 2110 JPEG XS

1. [プロトコル] には ST 2110 JPEG XS を選択します。
2. [VPC インターフェイス 1] では、コンテンツの送信先となる VPC インターフェイスのいずれかを選択し、出力の送信先となる特定の IP アドレスを選択します。

3. [VPC インターフェイス 2] では、コンテンツの送信先となる 2 番目の VPC インターフェイスを選択し、出力の送信先となる特定の IP アドレスを選択します。VPC インターフェイス 1 と 2 の間に優先順位はありません。
4. 出力の一部として送信するメディアストリームごとに、次の操作を行います。
   a. [メディアストリーム名] には、メディアストリームの名前を選択します。フロー上のソースが使用するメディアストリームのみを追加できます。
   b. [エンコーディング名] には、データのエンコードに使用された形式を選択します。
      - 補助データストリームの場合、エンコーディング名を **smpte291** に設定します。
      - オーディオストリームの場合、エンコーディング名を **pcm** に設定します。
      - ビデオの場合、エンコーディング名を **jxsv** に設定します。
   c. [ポート] には、この出力にコンテンツを配信するときに使用するポートを選択します。ポートの詳細については、「HTTP 送信先」を参照してください。
   d. [エンコーダプロファイル] には、圧縮の設定を選択します。このプロパティは、ソースが CDI プロトコルを使用する場合にのみ適用されます。
   e. [圧縮係数] には、出力の圧縮を計算する際にサービスが使用する値を指定します。有効な値は 3.0 ~ 10.0 までの浮動小数点数です。出力のビットレートは次のように計算されます。

      出力ビットレート = (1/圧縮係数) * (ソースのビットレート)

      このプロパティは、ソースが CDI プロトコルを使用する場合にのみ適用されます。
5. [出力の追加] を選択します。

フローの出力リストの表示

フローの出力リストと一緒に、各出力に関連付けられた設定を表示できます。このリストには、追加した出力とユーザーが付与した使用権限に基づいてサブスクライバーがフローを作成したときに、AWS Elemental MediaConnect が追加した出力が含まれています。

既存のフロー (コンソール) の出力リストを表示するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、表示するフローの名前を選択します。

   そのフローの詳細ページが表示されます。

3. [出力] タブを選択します。

   そのフローの出力リストが表示されます。

既存のフロー (AWS CLI) の出力リストを表示するには

- AWS CLI で、describe-flow コマンドを使用します。

```
aws mediaconnect describe-flow --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --
region us-east-1 --profile PMprofile
```

戻り値には、すべての出力を含むフロー全体の詳細が表示されます。戻り値の例を以下に示します。

```
{
  "Flow": {
    "AvailabilityZone": "us-east-1d",
    "Entitlements": [],
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "Name": "BasketballGame",
    "Outputs": [
      {
        "Address": "192.0.2.12",
        "Description": "RTP-FEC Output",
        "Name": "NYCOutput",
        "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:NYCOutput",
        "Port": 5020,
        "Protocol": "rtp-fec"
      },
      {
        "Address": "198.51.100.8",
        "Description": "RTP Output",
        "Name": "DCOutput",
        "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-987655dEF67hiJ89-c34de5fG678h:DCOutput",
        "Port": 5110,
        "Protocol": "rtp"
      }
    ],
```

```
    "Source": {
      "IngestIp": "195.51.100.21",
      "IngestPort": 5010,
      "Name": "BasketballGameSource",
      "Protocol": "rtp-fec",
      "SourceArn": "arn:aws:mediaconnect:us-
east-1:111122223333:source:3-4aBC56dEF78hiJ90-4de5fG6Hi78Jk:BasketballGameSource",
      "AllowlistCidr": "10.24.34.0/23"
    },
    "Status": "STANDBY"
  }
}
```

フローの出力の更新

フローがアクティブな場合でも、フローの出力を更新できます。

フロー (コンソール) の出力を更新するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、更新する出力に関連付けられたフローの名前を選択します。
3. [出力] タブを選択します。

   そのフローの出力リストが表示されます。
4. 更新する出力を選択します。
5. [更新] を選択します。
6. 適切な変更を行い、[保存] を選択します。

フロー出力 (AWS CLI) を更新するには

- AWS CLI で、update-flow-output コマンドを使用します。

```
aws mediaconnect update-flow-output --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --
output-arn "arn:aws:mediaconnect:us-east-1:111122223333:output:2-3aBC45dEF67hiJ89-
c34de5fG678h:NYCfeed" --port 5040 --region us-east-1 --profile PMprofile
```

戻り値の例を以下に示します。

```
{
  "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
  "Output": {
    "Address": "192.0.2.12",
    "Encryption": {
      "Algorithm": "aes256",
      "KeyType": "static-key",
      "RoleArn": "arn:aws:iam::111122223333:role/AllowMediaConnect",
      "SecretArn": "arn:aws:secretsmanager:us-west-2:111122223333:secret:SECRETID"
    },
    "Name": "Output1",
    "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:Output1",
    "Port": 5040,
    "Protocol": "rtp-fec"
  }
}
```

出力のタグの管理

タグを使用することで、AWS Elemental MediaConnect のフロー、ソース、出力、および使用権限の請求先や組織を追跡しやすくなります。これらは AWS 請求書の整理に AWS Billing and Cost Management が提供するものと同じタグです。コスト配分でタグがどのように使用されているかについては、「AWS Billingユーザーガイド」の「コスト配分タグを使用したカスタム請求レポート」を参照してください。

出力 (コンソール) へタグを追加するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを追加する出力に関連付けられたフローの名前を選択します。
3. [出力] タブを選択します。

   そのフローの出力リストが表示されます。
4. タグを追加する出力を選択します。
5. [タグを管理] を選択します。
6. [タグを管理] をもう一度選択し、[新しいタグを追加] を選択します。

7. 追加するタグごとに、以下が必要になります。

   a. キーと値を入力します。たとえば、キーを **sports**、値を **golf** にすることができます。

   b. [タグを追加] を選択します。

8. [更新] を選択します。

出力 (コンソール) のタグを編集するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを編集する出力に関連付けられたフローの名前を選択します。
3. [出力] タブを選択します。

   そのフローの出力リストが表示されます。
4. タグを編集する出力を選択します。
5. [タグ] タブで、[タグの管理] を選択します。
6. [タグの管理] を選択します。
7. 必要に応じて、タグを更新します。
8. [更新] を選択します。

出力 (コンソール) からタグを削除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを削除する出力に関連付けられたフローの名前を選択します。
3. [出力] タブを選択します。

   そのフローの出力リストが表示されます。
4. ユーザーを削除するグループを選択します。
5. [タグ] タブで、[タグの管理] を選択します。
6. [タグの管理] を選択します。
7. 削除するタグの横にある [タグの削除] を選択します。
8. [更新] を選択します。

フローからの出力の削除

フローに追加した出力を削除できます。AWS Elemental MediaConnect が使用権限の結果として出力を生成した場合は、使用権限を取り消す必要があります。

フロー (コンソール) から出力を削除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、削除する出力に関連付けられたフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [出力] タブを選択します。
4. 出力を選択してから、[削除] を選択します。

フロー (AWS CLI) から出力を削除するには

- AWS CLI で、`remove-flow-output` コマンドを使用します。

```
aws mediaconnect remove-flow-output --flow-arn "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame" --
output-arn "arn:aws:mediaconnect:us-east-1:111122223333:output:2-3aBC45dEF67hiJ89-
c34de5fG678h:Output1" --region us-west-2
```

戻り値の例を以下に示します。

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
    "OutputArn": "arn:aws:mediaconnect:us-
east-1:111122223333:output:2-3aBC45dEF67hiJ89-c34de5fG678h:Output1"
}
```

HTTP 送信先

フローの各出力は、異なる宛先に送信する必要があります。送信先を定義するパラメータはプロトコルによって異なりますが、どのプロトコルでも送信先の複合識別子が使用されます。たとえば、ポートが重複していない限り、複数の出力が同じ宛先の IP アドレスを指すことがあります。同様に、リ

モート ID が異なる限り、複数の出力が同じストリーム ID を指していてもかまいません。次のテーブルは、各プロトコルが送信先を定義する方法を示しています。

> **Note**
>
> 一部のプロトコルでは、エラー修正のために追加のポートが必要です。これらのプロトコルを使用する出力の場合、AWS Elemental MediaConnect は追加のポートを自動的に予約します。このプロトコルは、予約する必要のあるポートを具体的に定義します。たとえば、プロトコルによっては、エラー修正にポート番号 +2 とポート番号 +4 が必要です。出力にポート 5000 を指定すると、サービスによってポート 5000、5002、および 5004 が割り当てられます。

プロトコル	送信先の定義	必須ポート
CDI	各メディアストリームのポート	各メディアストリームに指定するポート。出力に必要なポートはこれだけです。
RIST	IP アドレス、ポート、およびポート +1	指定したポートと 1 つの追加ポート。このサービスは、指定したポート番号 +1 のポートを自動的に予約します。 たとえば、出力にポート 3000 を指定すると、サービスはポート 3001 も予約します。
RTP	IP アドレスとポート	指定するポート。出力に必要なポートはこれだけです。
RTP-FEC	IP アドレス、ポート、ポート +2、およびポート +4	指定したポートと 2 つの追加ポート。このサービスは、指定したポート番号 +2 および +4 のポートを自動的に予約します。

プロトコル	送信先の定義	必須ポート
		たとえば、出力にポート 2000 を指定すると、サービスはエラー修正用にポート 2002 と 2004 も予約します。
SRT リスナー	CIDR 許可リストとポート	指定するポート。出力に必要なポートはこれだけです。
SRT コーラー	IP アドレスとポート	指定するポート。出力に必要なポートはこれだけです。
Fujistu-QoS	CIDR 許可リストとポート	指定するポート。出力に必要なポートはこれだけです。
ST 2110 JPEG XS	各メディアストリームのポート	各メディアストリームに指定するポート。出力に必要なポートはこれだけです。
Zixi プル	ストリーム ID、リモート ID、および CIDR 許可リスト	サービスは、これらの出力に対して自動的にポート 2077 を使用します。
Zixi プッシュ	IP アドレス、ストリーム ID、およびポート	指定したポートは、出力に必要な唯一のポートです。

出力の IP アドレスの決定

リスナープロトコル (Zixi プルまたは SRT リスナーなど) を使用するフローの場合、レシーバーはフローとの接続を確立するために出力の IP アドレスを必要とします。

出力の IP アドレスを確認するには

1. [フロー] ページで、表示するフローの名前を選択します。
2. コンテンツが出力に送信される方法に基づく具体的な手順については、以下のタブから 1 つ選択してください

Public internet

1. [詳細] セクションで、パブリック送信 IP アドレスを書き留めます。これは、レシーバーに必要となる IP アドレスです。

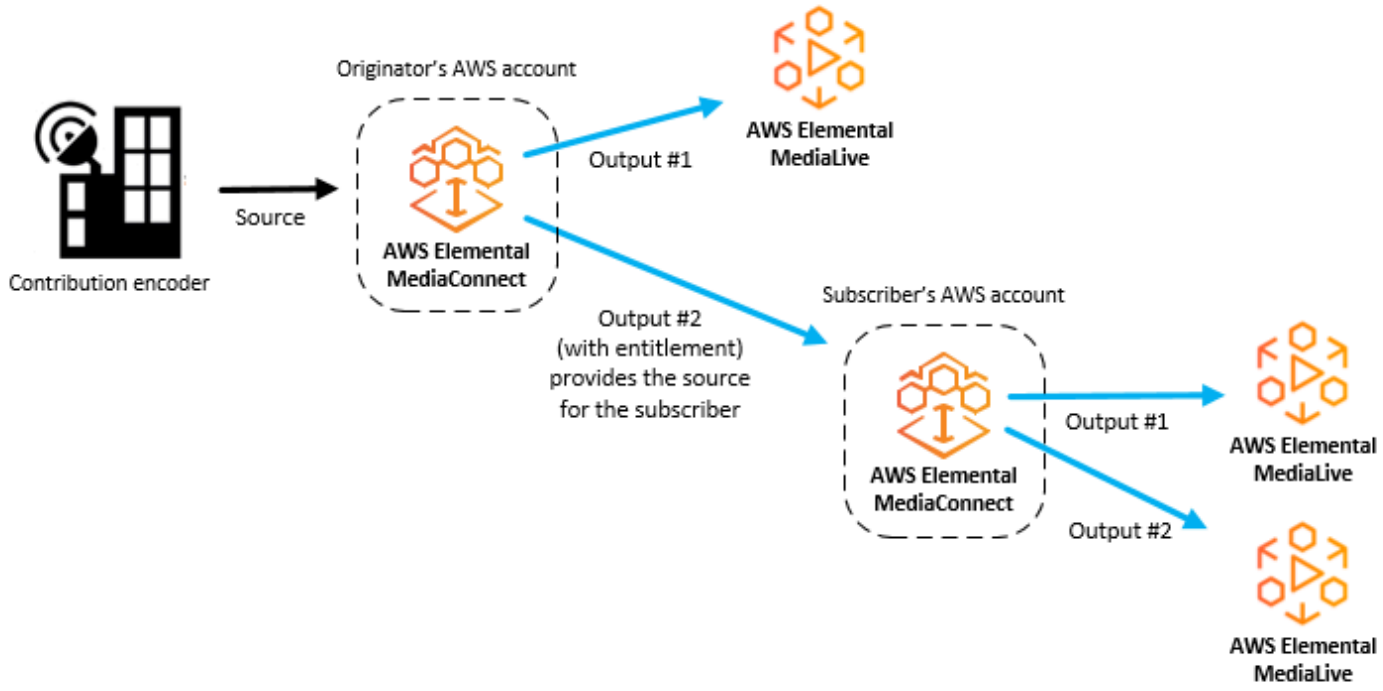
Private internet

1. [出力] タブを選択し、表示する出力を見つけます。
2. その出力の [リスナーアドレス] にある IP アドレスを書き留めます。これは、レシーバーに必要となる IP アドレスです。

AWS Elemental MediaConnect におけるエンタイトルメント

コンテンツ発信者は、自分のコンテンツを他の AWS アカウント (サブスクライバーアカウント) と共有するエンタイトルメントを付与できます。その後、サブスクライバーは、発信者のコンテンツをソースとして使用して独自の AWS Elemental MediaConnect フローを設定できます。次の図はこのプロセスを示しています。

> **Note**
>
> エンタイトルメントはトランスポートストリームフローでのみ付与できます。MediaConnect は CDI フローでのエンタイトルメントをサポートしていません。



トピック

- 他の AWS アカウントとコンテンツを共有する
- 別の AWS アカウントから提供されたコンテンツをサブスクライブする。

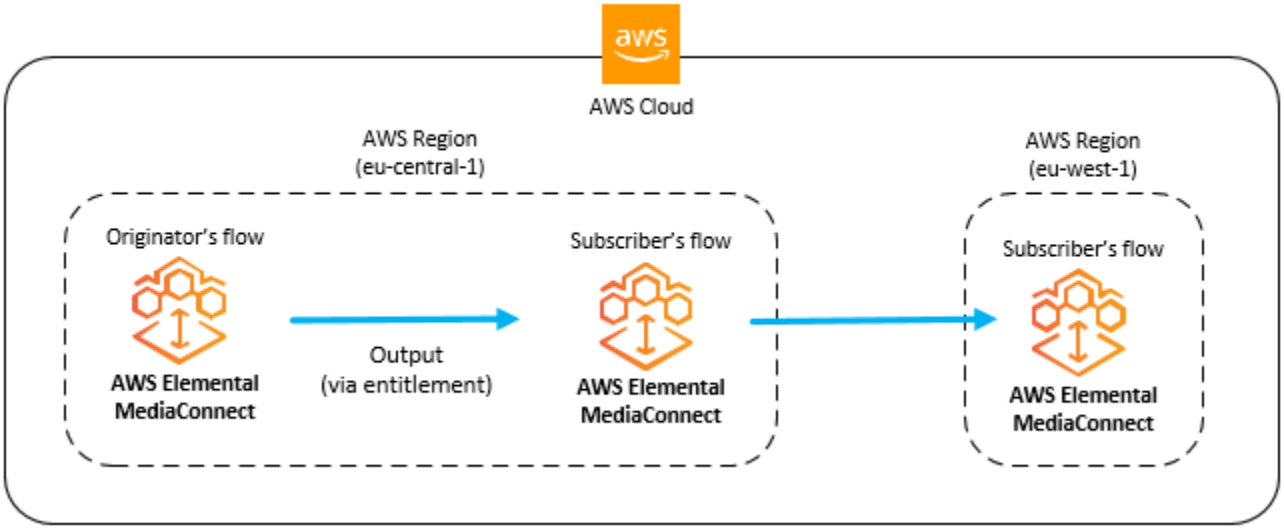
他の AWS アカウントとコンテンツを共有する

AWS Elemental MediaConnect フロー内のコンテンツを別の AWS アカウント (サブスクライバーアカウント) と共有するエンタイトルメントを付与できます。サブスクライバーがそのエンタイトルメントに基づいてフローを設定すると、サービスによって、自分のフローからサブスクライバーのフローへのストリームを代表するフロー出力が生成されます。この出力は、フローに含めることができる最大 50 件の出力の一部としてカウントされます。

アクティブなフロー上であっても、いつでもエンタイトルメントを付与、更新し、取り消すことができます。サブスクライバーのフローへのコンテンツのストリーミングを一時的に停止したい場合は、エンタイトルメントを無効にできます。後で、サブスクライバーのフローに再びコンテンツをストリーミングできるようにする準備ができたら、エンタイトルメントを有効化できます。サブスクライバーに負担させるエンタイトルメントデータ転送料金の割合を指定することもできます。

> **Note**
>
> エンタイトルメントを付与し、後で無効にして (サブスクライバーのフローへのコンテンツのストリーミングを一時的に停止する) 場合でも、そのエンタイトルメントはフローに関連付けられたままになり、エンタイトルメントの最大数にカウントされます。ただし、エンタイトルメントを取り消す (サブスクライバーのフローへのコンテンツのストリーミングを完全に停止する) と、そのエンタイトルメントはフローから削除され、エンタイトルメントの最大数にカウントされなくなります。

エンタイトルメントを付与したら、そのエンタイトルメントに関する情報 (名前、AWS リージョン、暗号化の詳細) をサブスクライバーに提供します。サブスクライバーはこの情報を使用して、あなたのフローをソースとして使用する MediaConnect フローを作成します。サブスクライバーのフローは、あなたのフローと同じ AWS リージョンに存在する必要があります。サブスクライバーが別のリージョン内のフローを希望する場合は、サブスクライバーが新しいリージョンで 2 つ目のフローを作成する必要があります。次の図はこのプロセスを示しています。



> **Note**
>
> エンタイトルメントはトランスポートストリームフローでのみ付与できます。MediaConnect は CDI フローでのエンタイトルメントをサポートしていません。

トピック

フローでのエンタイトルメントの付与

既存のフローにエンタイトルメントを付与して、コンテンツを別の AWS アカウント (サブスクライバーアカウント) と共有できます。サブスクライバーは、あなたのフローをソースとして使用して、同じ AWS リージョンに AWS Elemental MediaConnect フローを作成します。これが起きると、サービスは自分のフローからサブスクライバーのフローまでの動画ストリームを表す出力をフローに生成します。

サブスクライバーはエンタイトルメントを 1 回だけ使用できます。

前提条件

エンタイトルメントを付与するには、次の手順を行います。

- サブスクライバーの AWS アカウント番号を取得します。
- 自分のフローからサブスクライバーのフローに送信される動画を暗号化する場合は、静的キーの暗号化 または Secure Packager and Encoder Key Exchange (SPEKE) を使用して暗号化を設定します。

フロー (コンソール) にエンタイトルメントを付与するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、エンタイトルメントを付与するフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [実験] タブを選択します。
4. [エンタイトルメントを付与] を選択します。

   [エンタイトルメントを付与] ページが表示されます。
5. [名前] には、自分とサブスクライバーがこのフローを他のフローと区別するのに役立つ名前の名前を指定します。この名前は、サブスクライバーに表示されるエンタイトルメント ARN の一部にもなります。
6. [サブスクライバーアカウント ID] には、サブスクライバーの 12 桁のアカウント ID を指定します。AWSID にはハイフンを含めないでください。
7. [説明] には、この資格を後で識別するのに役立つ説明を指定します。この説明は、アカウントの AWS Elemental MediaConnect コンソールにのみ表示されます。
8. [サブスクライバーのデータ転送料金の割合] で、サブスクライバーに負担させるエンタイトルメントデータ転送料金の割合を指定します。AWS が残額をアカウントに請求します。たとえば、15 を指定すると、AWSエンタイトルメントデータ転送料金の 15% を利用者のアカウントに請求し、残りの 85% を自分のアカウントに請求します。

> **Note**
>
> エンタイトルメントデータ転送料金の一部または全部をサブスクライバーが負担するように指定しても、サブスクライバーはこのエンタイトルメントに基づくフローを作成して開始するまで料金が発生しません。

9. [エンタイトルメントステータス] では、エンタイトルメントを有効にするか無効にするかを指定します。エンタイトルメントが有効になっている場合、サブスクライバーはエンタイトルメントに基づいてフローを作成し、すぐにコンテンツのストリーミングを開始できます。エンタイトルメントが無効になっている場合、自分のフローからサブスクライバーのフローにコンテンツがストリーミングされるよう、サブスクライバーはエンタイトルメントを有効になるまで待機する必要があります。
10. 自分のフローからサブスクライバーのフローに送信される動画を暗号化する場合は、以下のタブのいずれかを選択します。

    Static key encryption

    1. [暗号化] セクションで [有効化] を選択します。
    2. [暗号化タイプ] には [静的キー] を選択します。
    3. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
    4. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。
    5. [暗号化アルゴリズム] には、ソースの暗号化に使用する暗号化の種類を選択します。

    SPEKE encryption

    1. [暗号化] セクションで 有効化 を選択します。
    2. [暗号化タイプ] には SPEKE を選択します。
    3. [暗号化アルゴリズム] には、ソースの暗号化に使用する暗号化の種類を選択します。
    4. [ロール ARN] で、API ゲートウェイを介してリクエストを送信するためのアクセス権限を付与する、IAM ロールの Amazon リソースネーム (ARN) を入力します。このロールは 暗号化を設定したときに作成しました。

       以下は、ロール ARN の例です。

       ```
       arn:aws:iam::111122223333:role/SpekeAccess
       ```

    5. [リソース ID] で、コンテンツの識別子を入力します。この ID は、現在のエンドポイントを特定するために、サービスよりキーサーバーに送信されます。この設定を、どの程度特有なものにするかは、どの程度詳細なアクセス制御を求めるかによって異なります。リソース ID は、コンテンツ ID とも呼ばれます。

       以下に、リソース ID の例を示します。

```
MovieNight20171126093045
```

6. デバイス I] で、条件付きアクセス (CA) プラットフォームのキープロバイダーで構成したデバイスの 1 つの値を入力します。
7. [URL] に、キーサーバーと通信するためにセットアップした API ゲートウェイプロキシの URL を入力します。API ゲートウェイプロキシ は、MediaConnect と同じ AWS リージョン に配置する必要があります。

   次は、その URL の例です。

   ```
   https://1wm2dx1f33.execute-api.us-west-2.amazonaws.com/SpekeSample/
   copyProtection
   ```

8. (オプション) [定数初期化ベクトル] に、コンテンツを暗号化するためのキーで使用される、128 ビット (16 バイト) の 16 進値を、32 文字の文字列により入力します。

11. ページの下部で、[権限を付与] を選択します。
12. [エンタイトルメント] タブのリストから新しいエンタイトルメントを探します。
13. エンタイトルメント ARN を書き留めます。
14. 次の情報をサブスクライバーに提供します。

    - エンタイトルメント ARN。
    - フローが作成された AWS リージョンです。
    - エンタイトルメントに暗号化を設定した場合の暗号化キーとアルゴリズム。
    - サブスクライバーに負担させるエンタイトルメントデータ転送料金の割合。

> **Note**
>
> MediaConnect は、コンテンツ発信者のフローとサブスクライバーのフロー間のデータ接続を最適化するために、ヌルパケットを抑制します。その結果、サブスクライバーのフローのビットレートが変動したり、コンテンツ発信者のフローとサブスクライバーのフローのビットレートの間で違いが生じたりする可能性があります。ソースの健全性は、SourceBitRate と、SourceContinuityCounter や SourceNotRecoveredPackets などの他のメトリクスを組み合わせてモニタリングすることをお勧めします。

フロー (AWS CLI) に権限を付与するには

1. 付与するエンタイトルメントの詳細を含む JSON ファイルを作成します。

   次の例では、ファイルのコンテンツを示します。

```
[
  {
    "Description": "For AnyCompany",
    "Encryption": [
      {
        "Algorithm": "aes128",
        "KeyType": "static-key",
        "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
        "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1"
      }
    ],
    "Name": "AnyCompany_Entitlement",
    "Subscribers": [
      "444455556666",
      "123456789012"
    ]
  },
  {
    "Description": "For Example Corp",
    "Name": "ExampleCorp",
    "Subscribers": [
      "777788889999"
    ]
  }
]
```

2. AWS CLI で、`grant-flow-entitlements` コマンドを使用します。

```
aws mediaconnect grant-flow-entitlements --entitlements --flow-
arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame  --cli-input-
json file://entitlements.json
```

   戻り値の例を以下に示します。

```
{
    "Entitlements": [
        {
            "Name": "AnyCompany_Entitlement",
            "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement",
            "Subscribers": [
                "444455556666", "123456789012"
            ],
            "Description": "For AnyCompany",
            "Encryption": {
                "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1",
                "Algorithm": "aes128",
                "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
                "KeyType": "static-key"
            }
        },
        {
            "Name": "ExampleCorp",
            "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-3333cccc4444dddd-1111aaaa2222:ExampleCorp",
            "Subscribers": [
                "777788889999"
            ],
            "Description": "For Example Corp"
        }
    ],
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame"
}
```

エンタイトルメントの更新

エンタイトルメントを作成した後でも、説明、ステータス、サブスクライバーを更新できます。サブスクライバーアカウント ID を変更すると、当初のサブスクライバーアカウントではコンテンツを利用できなくなります。当初のサブスクライバーがエンタイトルメントをソースとして使用するフローをすでに作成している場合、関連付けられた出力はフローから削除されます。

エンタイトルメント (コンソール) を更新するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、更新するエンタイトルメントに関連付けられたフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [実験] タブを選択します。
4. 更新するエンタイトルメントを選択します。
5. [更新] を選択します。
6. 適切な変更を行い、[保存] を選択します。

フロー上のエンタイトルメントを更新するには (AWS CLI)

- AWS CLI で、`update-flow-entitlement` コマンドを使用します。

```
aws mediaconnect update-flow-entitlement --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame --
entitlement-arn arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement
 --description 'For AnyCompany Affiliate' --subscribers 444455556666",
 "123456789012
```

戻り値の例を以下に示します。

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "Entitlement": {
        "Name": "AnyCompany_Entitlement",
        "Description": "For AnyCompany Affiliate",
        "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement",
        "Encryption": {
            "KeyType": "static-key",
            "Algorithm": "aes128",
            "RoleArn": "arn:aws:iam::111122223333:role/MediaConnect-ASM",
            "SecretArn": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:mySecret1"
        },
        "Subscribers": [
```

```
            "444455556666", "123456789012"
        ]
    }
}
```

エンタイトルメントのタグ管理

タグを使用することで、AWS Elemental MediaConnect のフロー、ソース、出力、および使用権限の請求先や組織を追跡しやすくなります。これらは AWS 請求書の整理に AWS Billing and Cost Management が提供するものと同じタグです。コスト配分でタグがどのように使用されているかについては、「AWS Billingユーザーガイド」の「コスト配分タグを使用したカスタム請求レポート」を参照してください。

エンタイトルメント (コンソール) にタグを追加するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを追加するエンタイトルメントに関連付けられたフローの名前を選択します。
3. [実験] タブを選択します。

   そのフローのエンタイトルメントのリストが表示されます。
4. 更新するエンタイトルメントを選択します。
5. [タグの管理] を選択します。
6. [タグの管理] を選択し、[タグを追加] を選択します。
7. 追加するタグごとに、以下が必要になります。

   a. キーと値を入力します。たとえば、キーを **sports**、値を **golf** にすることができます。

   b. [タグを追加] を選択します。
8. [更新] を選択します。

エンタイトルメント (コンソール) のタグを編集するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを編集するエンタイトルメントに関連付けられたフローの名前を選択します。
3. [実験] タブを選択します。

そのフローのエンタイトルメントのリストが表示されます。

4. タグを編集するエンタイトルメントを選択します。
5. タグ タブで、タグの管理 を選択します。
6. [タグの管理] を選択します。
7. 必要に応じて、タグを更新します。
8. [更新] を選択します。

エンタイトルメント (コンソール) のタグを削除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、タグを削除するエンタイトルメントに関連付けられたフローの名前を選択します。
3. [実験] タブを選択します。

そのフローのエンタイトルメントのリストが表示されます。

4. タグを削除するエンタイトルメントを選択します。
5. [タグ] タブで、[タグの管理] を選択します。
6. [タグの管理] を選択します。
7. 削除するタグの横にある タグの削除 を選択します。
8. [更新] を選択します。

エンタイトルメントの取り消し

エンタイトルメントを取り消すと、サブスクライバーアカウントはそのコンテンツを永久に閲覧できなくなります。エンタイトルメントとそれに関連付けられた出力はフローから削除されます。エンタイトルメントを取り消し、後ほどそのエンタイトルメントを再度付与する必要があると判断した場合は、サブスクライバーのフローを手動で再開する必要があります。エンタイトルメントが付与されても、サブスクライバーのフローは自動的には開始されません。

サブスクライバーのフローへのコンテンツのストリーミングを一時的に停止したい場合は、エンタイトルメントを無効にしてください。

エンタイトルメント (コンソール) の取り消しを行う

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。

2. [フロー] ページで、取り消すエンタイトルメントに関連付けられたフローの名前を選択します。

   そのフローの詳細ページが表示されます。

3. [実験] タブを選択します。
4. 取り消すエンタイトルメントを選択します。
5. [取り消す] を選択します。

フロー上のエンタイトルメントを取り消すには (AWS CLI)

- AWS CLI で、`revoke-flow-entitlement` コマンドを使用します。

```
aws mediaconnect revoke-flow-entitlement --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame --
entitlement-arn arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement
```

戻り値の例を以下に示します。

```
{
    "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BaseballGame",
    "EntitlementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:entitlement:1-11aa22bb11aa22bb-3333cccc4444:AnyCompany_Entitlement"
}
```

エンタイトルメントを一時的に無効にする

エンタイトルメントを無効にすると、そのコンテンツはサブスクライバーアカウントですぐに使用できなくなります。ただし、エンタイトルメントと関連付けられた出力はフローに残ります。これらのリソースは引き続きアウトプットとエンタイトルメントのクォータにカウントされます。その後、エンタイトルメントを有効化してアクセスを回復できます。

サブスクライバーのフローへのコンテンツのストリーミングを永久に停止したい場合は、エンタイトルメントを取り消してください。このアクションにより、エンタイトルメントとそれに関連付けられた出力がフローから削除されます。

エンタイトルメント (コンソール) を無効にするには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、無効にするエンタイトルメントに関連付けられたフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [実験] タブを選択します。
4. 無効にするエンタイトルメントを選択します。
5. [無効化] を選択します。

一時的に無効化されたエンタイトルメントを有効にする

エンタイトルメントが無効になっている場合は、そのエンタイトルメントを有効にして、サブスクライバーのフローへのコンテンツのストリーミングを再開できます。

> **Note**
>
> エンタイトルメントが取り消された場合は、有効にすることはできません。新しいエンタイトルメントを付与する必要があります。

エンタイトルメント (コンソール) を有効にするには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. [フロー] ページで、有効にするエンタイトルメントに関連付けられたフローの名前を選択します。

   そのフローの詳細ページが表示されます。
3. [実験] タブを選択します。
4. 有効にするエンタイトルメントを選択します。
5. [有効化] を選択します。

別の AWS アカウントから提供されたコンテンツをサブスクライブする。

別の AWS アカウント (発信者アカウント) が自分の AWS アカウント (サブスクライバーアカウント) にエンタイトルメントを付与すると、発信者のコンテンツをソースとして使用するフローを作成できます。別の AWS アカウントから提供されたコンテンツをサブスクライブするには、自分に付与されたエンタイトルメントに基づいてフローを作成します。発信者のフローと同じ AWS リージョンにフローを設定する必要があります。

エンタイトルメントは 1 回だけ使用できます。

> **Note**
>
> MediaConnect は、コンテンツ発信者のフローとサブスクライバーのフロー間のデータ接続を最適化するために、ヌルパケットを抑制します。その結果、サブスクライバーのフローのビットレートが変動したり、コンテンツ発信者のフローとサブスクライバーのフローのビットレートの間で違いが生じたりする可能性があります。ソースの健全性は、`SourceBitRate` と、`SourceContinuityCounter` や `SourceNotRecoveredPackets` などの他のメトリクスを組み合わせてモニタリングすることをお勧めします。

前提条件

フローを作成する前に、以下の操作を行う必要があります。

- コンテンツの発信者から次の情報を入手します。
  - エンタイトルメント ARN。
  - 発信者がフローを作成した AWS リージョン
  - 発信者がエンタイトルメントに暗号化を設定した場合、暗号化キーとアルゴリズム
- エンタイトルメントが [静的キーによる暗号化] を使用して暗号化されている場合は、この手順を開始する前に AWS Secrets Manager に暗号化キーを保存してください。(コンテンツが SPEKE を使用して暗号化されている場合は、暗号化の設定のために何も行う必要はありません)。

エンタイトルメント (コンソール) に基づいてフローを作成するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。

2. 発信者のフローがあるのと同じ AWS リージョンにログインしていることを確認します。
3. [フロー] ページで [フローを作成] を選択します。
4. [詳細] セクションの [名前] で、フローの名前を指定します。
5. [アベイラビリティーゾーン] で、フローのアベイラビリティーゾーンを選択します。これは、発信者のフローのアベイラビリティーゾーンと一致している必要はありません。
6. [ソース] セクションで、[ソースタイプ] として [使用権限のあるソース] を選択します。
7. エンタイトルメント ARN では、適切なエンタイトルメントを選択します。このリストには、自分に与えられたすべての使用権限が含まれます。

> **Tip**
>
> このフィールドをクリックして、エンタイトルメント名の入力を開始できます。AWS Elemental MediaConnect は、入力した内容と一致する名前のエンタイトルメントのみを含むようにリストをフィルタリングします。

> **Note**
>
> ユーザーが負担するエンタイトルメントデータ転送料金の割合は、各エンタイトルメントの横に表示されます。この値はコンテンツ発信者が設定します。

8. 発信者が使用権限に暗号化を設定した場合は、[復号化] セクションで [有効化] を選択し、次の操作を行います。
   a. [復号化タイプ] には、静的キーを選択します。
   b. [ロール ARN] には、暗号化を設定したときに作成したロールの ARN を指定します。
   c. [シークレット ARN] には、暗号化キーを保存するシークレットを作成したときに AWS Secrets Manager が割り当てた ARN を指定します。
   d. [復号化アルゴリズム] では、発信者が提供した暗号化のタイプを選択します。
9. ページの下部で、[今すぐ作成] を選択します。

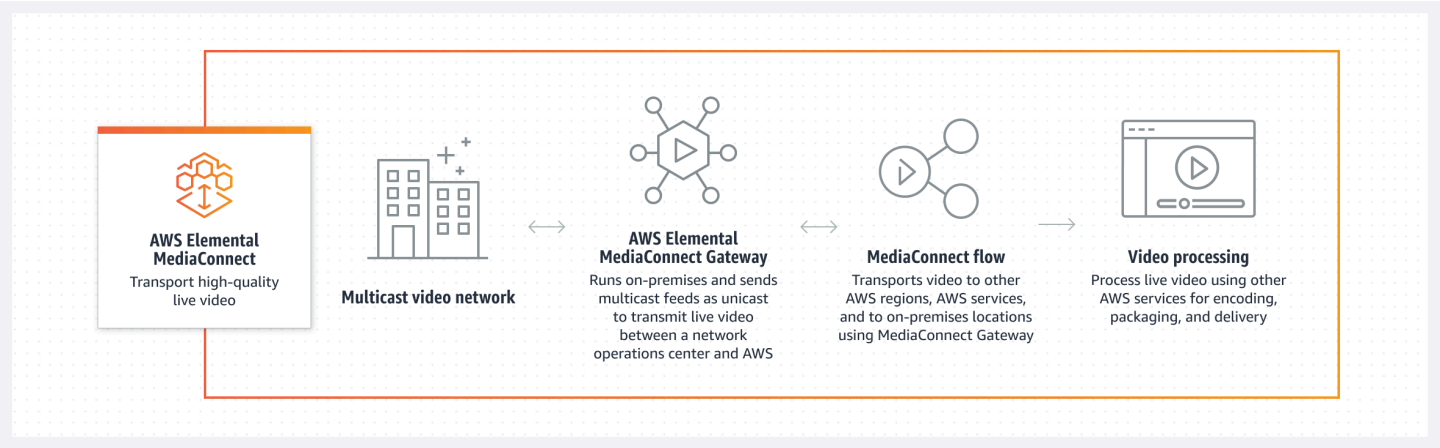
> **Note**
>
> フローは、自動的には開始されません。手動でフローを開始する必要があります。

10. 出力を追加して AWS Elemental MediaConnect にコンテンツを送信する場所を指定するか、他の AWS アカウントのユーザーがコンテンツをサブスクライブできるようにエンタイトルメントを付与します。

AWS Elemental MediaConnect Gateway

AWS Elemental MediaConnect Gatewayは、ライブビデオを AWS クラウド との間で転送するために、オンプレミスのリソースをデプロイする MediaConnect の機能です。MediaConnect Gateway を使用すると、AWS クラウドオンプレミスのハードウェアから にライブビデオを配信したり、AWS クラウド からローカルデータセンターにライブビデオを配信したりできます。

次の図は、AWS Elemental MediaConnect Gateway がオンプレミスで実行され、マルチキャストフィードをユニキャストとして送信するワークフローを示しています。このプロセスでは、オンプレミスのオペレーションセンターと AWS クラウド との間でライブビデオが送信されます。そこから、AWS Elemental MediaConnect Gateway は同じコンテンツを別のオンプレミスの場所に配信します。



このセクションでは、次のトピックについて説明します。

- 前提条件：MediaConnect Gateway を使用する際のオンプレミスシステム情報およびその他の考慮事項。
- MediaConnect Gateway のコンポーネント：MediaConnect Gateway とそのコンポーネントについて説明します。
- ゲートウェイの作成： ゲートウェイとそのコンポーネントを構築するためのステップバイステップの手順。

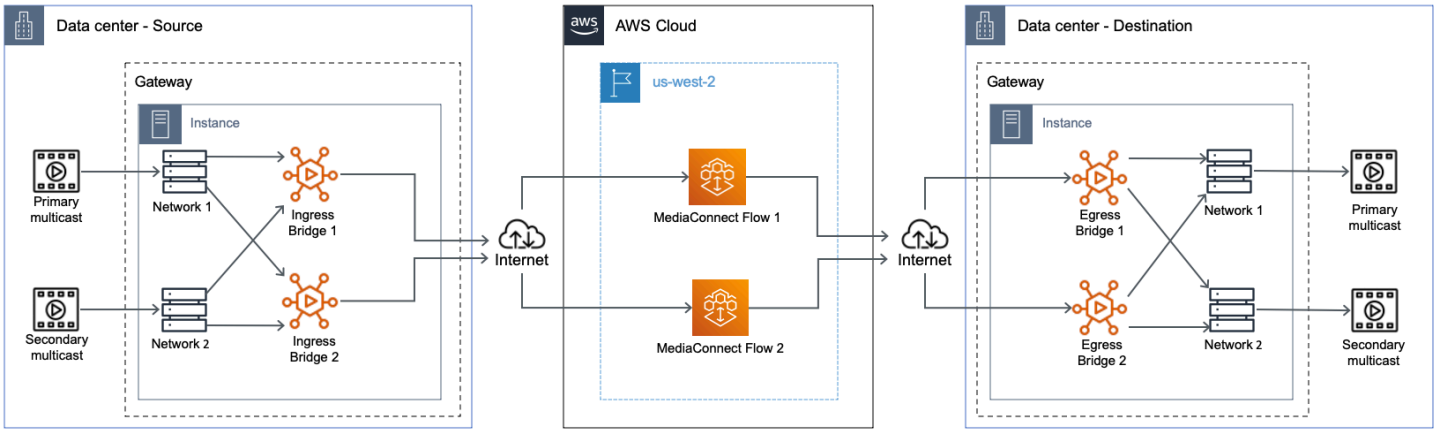
MediaConnect Gateway のコンポーネント

AWS Elemental MediaConnect Gateway は、ゲートウェイ、ネットワーク、インスタンス、ブリッジという 4 つの主要コンポーネントで構成されています。各コンポーネントについては、本ガイド

の以下のセクションで詳しく説明します。以下に、これらのコンポーネントの基本的な関係について説明します。

- ゲートウェイは、インスタンスとブリッジを論理的にグループ化したものです。各ゲートウェイは、データセンターと AWS クラウド 間の通信にユーザー定義の IP 情報を活用します。
- ネットワーク：MediaConnect Gateway ネットワークは、インスタンスとブリッジがローカルデータセンターネットワーク上で通信するために使用する IP 情報の集まりです。ネットワーク情報は、ゲートウェイとの通信に使用しているローカルデータセンターネットワークと一致する必要があります。各 MediaConnect Gateway には、最大 2 つのネットワークを含めることができます。すべてのゲートウェイには、少なくとも 1 つのネットワークを含める必要があります。
- インスタンス：データセンターの機器上で実行され、MediaConnect によって管理されるコンピューティングインスタンス。このインスタンスは MediaConnect サービスのオンプレミス実装であり、ゲートウェイ内に含まれています。インスタンスはブリッジを使用してデータセンターと AWS クラウド の間で通信します。オンプレミスサーバーにソフトウェアをインストールして、インスタンスを作成します。
- ブリッジ：データセンターのインスタンスと AWS クラウド との間の接続です。ブリッジを使用して、 AWS クラウド からデータセンターへ、またはデータセンターから AWS クラウド へビデオを送信できます。

次の図は、一般的なワークフローシナリオにおける各コンポーネントの相互作用を示しています。このワークフローでは、データセンターからのマルチキャストがゲートウェイのインスタンスに取り込まれ、ブリッジを介して AWS クラウド 内の MediaConnect に送信されます。マルチキャストは AWS クラウド から、別のデータセンターのゲートウェイのインスタンスに配信されます。



MediaConnect Gateway の用語

次のセクションでは、MediaConnect Gateway の概念と用語について詳しく説明します。

- イングレス：MediaConnect Gateway では、イングレスとはオンプレミスの場所から AWS クラウド に投稿されたコンテンツを指します。コンテンツがイングレスブリッジを使用してロケーションから送信される場合、その送信先は AWS であることを意味します。
- エグレス：MediaConnect Gateway では、エグレスとは、 AWS クラウド からオンプレミスの場所に配信されるコンテンツを指します。コンテンツがエグレスブリッジを使用してお客様のロケーションに入ってくる場合、ソースは AWS であることを意味します。
- クラウドフロー：AWS クラウド に存在するMediaConnect フロー。通常、これはすでに使用していて、オンプレミスのゲートウェイに配信したい既存の MediaConnect フローです。
- フローソース：AWS クラウド を起点とするソース。エグレスブリッジはこのタイプのソースを使用します。
- ネットワークソース：オンプレミスのロケーションを起点とするソース。イングレスブリッジはこのタイプのソースを使用します。
- フロー出力：AWS クラウド に配信される出力。イングレスブリッジはこのタイプの出力を使用します。
- ネットワーク出力：オンプレミスの場所に配信される出力。エグレスブリッジはこのタイプの出力を使用します。

前提条件

AWS Elemental MediaConnect Gateway を使用するには、事前に AWS アカウント アカウントが必要です。また、MediaConnect Gateway コンポーネントにアクセスし、表示や編集を行うための適切なアクセス許可が必要です。さらに、以下のセクションに記載されている MediaConnect Gateway の要件を満たす物理ハードウェアが必要になります。

サポートされるオペレーティングシステムとシステムアーキテクチャ

一般情報

AWS Elemental MediaConnect Gateway は Amazon Elastic Container Service Anywhere (ECS Anywhere) サービスをベースに構築されています。Amazon ECS Anywhere は、オンプレミスサーバーなどの外部インスタンスを AWS インフラストラクチャに登録するためのサポートを提供します。このアーキテクチャのため、MediaConnect Gateway を使用する外部インスタンスは Amazon ECS Anywhere の要件と、MediaConnect Gateway 専用の追加要件に準拠する必要があります。以下のセクションでは、MediaConnect Gateway 固有の要件に加えて、ハードウェアとオペレーティングシステム (OS) の要件を一覧表示します。

次の表は、各 MediaConnect Gateway コンポーネントのデフォルトクォータを示しています。

コンポーネント	デフォルトのクォータ	クォータを増やすことはできますか？
AWS リージョン ごとのゲートウェイの最大数	3	Yes
各ゲートウェイのインスタンスの最大数	20	No
各ゲートウェイのブリッジの最大数	40	No
各ブリッジの最大ビットレート	100 Mbps	No

サポート対象のシステムアーキテクチャ

以下の表には、個々のゲートウェイのインスタンスに推奨されるシステムアーキテクチャが記載されています。システムは、インスタンスで実行できるブリッジの最大数を決定します。x86_64 CPU アーキテクチャのみがサポートされています。ARM ベースの CPU は MediaConnect Gateway によってサポートされていません。

ブリッジ数	vCPU コア (2.6 GHz)	vCPU コア (3.0 GHz)	最小 RAM (GB)	最小ディスクスペース (GB)
10	2	2	4	25
25	6	4	8	25
40	10	8	16	25

CPU リファレンス

CPU アーキテクチャは次の CPU を使用してベンチマークされています。

- 2.6 GHz - Intel E5-2660 v3

- 3.0 GHz - AMD 7302

サポートされるオペレーティングシステム

次のリストには、MediaConnect Gateway インスタンスでサポートされているオペレーティングシステム (OS) とソフトウェア構成が含まれています。

推奨オペレーティングシステム

- RedHat Enterprise Linux (RHEL) 8-OS は RedHat サポート契約で定められている最新のパッチを適用し続ける必要があります。

サポートされるオペレーティングシステム

MediaConnect Gateway インスタンスは、Amazon ECS Anywhere でサポートされている他の Linux ディストリビューションに登録できます。Windows オペレーティングシステムはMediaConnect Gateway ではサポートされていません。サポートされている Linux ディストリビューションの全リストについては、「Amazon ECS ユーザーガイド」の「サポートされているオペレーティングシステム」を参照してください。

必要なソフトウェア

- Docker-MediaConnect Gateway では、Docker の最新リリースをインストールする必要があります。RHEL 以外の Linux ディストリビューションを使用している場合は、MediaConnect が提供するインスタンス登録スクリプトによって Docker がインストールされます。DockerまたはRHELのオープンパッケージリポジトリのいずれも、RHELにDockerをネイティブにインストールすることはできません。このドキュメントで説明されているインストールスクリプトを実行する前に、Docker がインストールされていることを確認する必要があります。

ネットワーク

ゲートウェイネットワークは、ローカル データセンター ネットワーク上で通信するためにインスタンスとブリッジによって使用される IP 情報の集合です。ゲートウェイネットワーク情報は、ゲートウェイとの通信に使用しているローカルデータセンターネットワークと一致する必要があります。各ゲートウェイには、最大 2 つのネットワークを含めることができます。すべてのゲートウェイには、少なくとも 1 つのネットワークを含める必要があります。

ゲートウェイネットワークの作成または削除

ネットワークは、新しいゲートウェイを初めて作成するときに作成する必要があります。ゲートウェイを最初に作成した後は、ネットワークを追加したり編集したりすることはできません。ゲートウェイとそのネットワークの初期作成の詳細については、「ゲートウェイ (コンソール) の作成」を参照してください。

ネットワークを削除するには、そのネットワークに関連付けられているゲートウェイを削除する必要があります。ゲートウェイとそのネットワークの削除の詳細については、「ゲートウェイとそのコンポーネントの削除 (コンソール)」を参照してください。

インスタンス

インスタンスはデータセンターの機器上で実行され、 MediaConnect Gatewayによって管理されるコンピューティングインスタンスです。このインスタンスは MediaConnect サービスのオンプレミス実装であり、ゲートウェイ内に含まれています。インスタンスはブリッジを使用してデータセンターと AWS クラウド の間で通信します。インスタンスは、オンプレミスサーバーにソフトウェアをインストールすることによって作成されます。

MediaConnect Gateway インスタンスの登録

インスタンスをホストするデバイス上でカスタム Linux コマンドを実行することで、インスタンスを登録できます。コマンドは、AWS マネジメントコンソール のインスタンス登録プロセスに従って生成します。

MediaConnect Gateway インスタンスの登録

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、インスタンスを登録するゲートウェイを選択します。
3. ゲートウェイの 詳細 ページで、インスタンス タブを選択します。インスタンスを登録 を選択します。
4. ゲートウェイインスタンスの登録 ページで、次のステップを完了します。

    1. アクティベーションキーの期間を使用する場合、アクティベーションキーがアクティブなままになる日数を入力します。その日数が経過すると、ゲートウェイのインスタンスを登録する際にキーは機能しなくなります。

2. インスタンス数を使用する場合　アクティベーションキーを使用してクラスターに登録する外部インスタンスの数を入力します。
3. インスタンスロールを使用する場合、外部インスタンスに関連付ける IAM ロールを選択します。
4. 登録コマンドを生成 を選択します。

5. Linux コマンドが表示されます。COPY コマンドをコピーします。このコマンドは、このゲートウェイに登録する各インスタンスで実行する必要があります。

> **Important**
>
> スクリプトの bash 部分は root として実行する必要があります。コマンドが root として実行されない場合、エラーが返されます。

6. 数分後、インスタンスはゲートウェイに登録されます。このゲートウェイに登録されているすべてのインスタンスがインスタンス タブに表示されます。

ゲートウェイのインスタンスの登録解除

使用しなくなったインスタンスは、MediaConnect Gateway 内で登録を解除することができます。インスタンスを登録解除すると、ブリッジはサポートされなくなり、ゲートウェイの一部ではなくなります。インスタンスを Amazon ECS Anywhere または別のゲートウェイのインスタンスとして再利用する場合は、ステップ 6の追加手順に従って、登録解除されたインスタンスを再利用できるように準備する必要があります。

ゲートウェイのインスタンスを登録解除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、登録解除するインスタンスを含むゲートウェイを選択します。
3. ゲートウェイの 詳細 ページで、インスタンス タブを選択します。登録解除するインスタンスのインスタンス ID を選択します。
4. 登録解除 を選択します。
5. インスタンスの登録解除 を選択してインスタンスの登録解除を確定します。
6. 登録解除する必要のある追加のインスタンスについては、前のステップを繰り返します。

ゲートウェイのインスタンスを再利用するには (オプション)

インスタンスを Amazon ECS Anywhere または別のゲートウェイのインスタンスとして再利用する場合は、次のステップを完了する必要があります。

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、再利用するインスタンスを含むゲートウェイを選択します。
3. ゲートウェイの 詳細 ページで、インスタンス タブを選択します。再起動するインスタンスのインスタンス ID を追加します。
4. 再利用するインスタンスのインスタンスのステータス が登録解除 になっていることを確認します。
5. アクセス権を持つコンピューターから、SSH を使用してインスタンスに接続します。
6. 次の各コマンドを順番に実行します。

```
sudo docker stop $(docker ps -f "name=MediaConnectGatewayAgent" -q); \
sudo docker stop ecs-agent; \
sudo systemctl stop ecs amazon-ssm-agent; \
sudo yum remove -y amazon-ecs-init amazon-ssm-agent;  `# or apt or snap as needed`
 \
sudo rm /var/lib/ecs /etc/ecs /var/lib/amazon/ssm /var/log/ecs /var/log/amazon/ssm
 -rf; \
sudo docker rm -f ecs-agent ssm-agent; \
sudo docker container rm -f $(docker ps -a -f "name=MediaConnectGatewayAgent" -q);
 \
sudo docker volume rm -f ecsdata docker run; \
sudo pkill -f -KILL network_bootstra[p]; \
sudo pkill -KILL mcproxy;
```

MediaConnect Gateway とそのネットワークの削除の詳細については、「ゲートウェイとそのコンポーネントの削除 (コンソール)」を参照してください。

ブリッジ

ブリッジは、データセンターのインスタンスとAWS クラウド をつなぐ接続です。選択したブリッジタイプに応じて、ブリッジを使用して AWS クラウド からデータセンターに、またはデータセンターから AWS クラウド にコンテンツを送信できます。

ブリッジのタイプ

AWS Elemental MediaConnect Gatewayは、2 種類のブリッジをサポートしています。各ブリッジタイプは異なる目的を果たし、コンテンツを AWS クラウド に提供するか、物理的な場所にコンテンツを配布するかを決定します。2 つのタイプのブリッジとそれぞれの機能を次に示します。

イングレスブリッジ：グラウンドからクラウドへのブリッジ。イングレス ブリッジでは、コンテンツは施設で発信され、AWS クラウド に配信されます。

エグレスブリッジ：クラウドからグラウンドへのブリッジ。エグレスブリッジでは、コンテンツは既存の MediaConnect フローから取得され、施設に配信されます。

ブリッジソース

各ブリッジでは、少なくとも 1 つのソースを作成する必要があります。ソースは、MediaConnect Gateway によって取り込まれるコンテンツです。ソースコンテンツの配信元は、選択したブリッジタイプによって異なります。複数のブリッジソースを作成する場合、作成プロセス中にフェールオー

バーを有効にすることで、ブリッジの回復力を高めることができます。ソースは次の 2 種類があります。

- イングレスブリッジリソース：イングレスブリッジの場合、コンテンツは施設で送信され、クラウドに配信されます。イングレスブリッジソースを作成するときは、プロトコル (RTP、RTP-FEC、UDP) を選択し、施設で送信されるコンテンツのマルチキャスト IP アドレスとポートを入力する必要があります。
- エグレスブリッジソース：エグレスブリッジの場合、コンテンツは既存の MediaConnect フローとして送信され、施設に配信されます。エグレスブリッジソースを作成するときは、施設に送信したいMediaConnect フローを選択する必要があります。プロトコルを選択する必要はありません。ソースは、既存のフローと同じプロトコルを使用します。

ブリッジソースのフェイルオーバー

複数のブリッジソースを作成する場合、作成プロセス中にフェールオーバーを有効にすることで、ブリッジの回復力を高めることができます。フェイルオーバー設定は、ソースインプットが失われた場合の AWS Elemental MediaConnect Gateway の動作を決定します。ブリッジタイプによって、2 つのフェイルオーバーモードのどちらが使用できるかが決まります。2 つのフェイルオーバーモードは次のとおりです。

- フェールオーバー：このモードでは、プライマリソースとバックアップソースを切り替えることができます。ソースをプライマリソースとして指定できます。2 つ目のソースはバックアップとして機能します。プライマリソースに障害が発生すると、サービスはバックアップソースに切り替わり、信頼性が確保され次第、プライマリソースに戻ります。
- マージ：このモードでは、ソースストリームを 1 つのストリームに結合するので、単一ソースの損失から正常に回復できます。マージモードでは、送信元にパケットがないと、サービスは失われたパケットをもう一方の送信元から引き出します。

ブリッジ出力

各ブリッジでは、少なくとも 1 つの出力を作成する必要があります。出力は次の 2 種類があります。

- イングレスブリッジ出力：イングレスブリッジの場合、コンテンツは施設で送信され、クラウドに配信されます。イングレスブリッジタイプの出力を設定する必要はありません。イングレスブリッジをソースとして使用して MediaConnect フローを作成すると、フローの開始時に出力が自動的に作成されます。

- エグレスブリッジソース：エグレスブリッジの場合、コンテンツは既存の MediaConnect フローとして送信され、お客様の施設に配信されます。エグレスブリッジ出力を作成する場合、施設に配信される IP とプロトコルの情報を設定する必要があります。エグレスブリッジエグレスは RTP、RTP-FEC、および UDP プロトコルをサポートします。

MediaConnect Gateway ブリッジの作成

少なくとも 1 つのインスタンスをゲートウェイに登録したら、ブリッジを作成できます。ブリッジを作成するプロセスは、ステップ 4 で選択したブリッジタイプによって異なります。

イングレスブリッジを作成するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、ブリッジを作成するゲートウェイを選択します。
3. ゲートウェイ詳細 ページで、ブリッジ タブを選択します。ブリッジの作成 を選択します。
4. ブリッジの作成 ページの詳細 セクションで次の手順を実行します。
    1. ブリッジの 名前 を入力します。
    2. ブリッジタイプ として、イングレスブリッジ を選択します。
    3. ブリッジ経由で転送するコンテンツの最大ビットレート を入力します。
    4. ブリッジの 最大出力 を入力します。
5. 次に、ソース セクションで以下の手順を実行します。イングレスブリッジのソースは、施設で送信されるマルチキャストコンテンツです。ソースを作成するには：
    1. ソースの 名前 を入力します。
    2. ネットワーク を選択します。これはゲートウェイのセットアッププロセス中に作成したネットワークです。
    3. ソースコンテンツの プロトコル を選択します。
    4. ソースのマルチキャスト IP とポート を入力します。
6. 複数のソースを追加する場合は、フェイルオーバー設定 セクションでフェイルオーバーを設定できます。
    a. フェイルオーバーモード としてフェイルオーバー またはマージ を選択する
    b. モードとして フェイルオーバー を選択した場合は、ステップ 5 で設定したソースの 1 つをプライマリソース として選択します。

7. ブリッジの作成 を選択します。
8. ブリッジが作成されたら、ブリッジの 詳細 ページで 開始 を選択してブリッジを起動できます。

エグレスブリッジを作成するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、ブリッジを作成するゲートウェイを選択します。
3. ゲートウェイ詳細 ページで、ブリッジ タブを選択します。ブリッジの作成 を選択します。
4. ブリッジの作成 ページの詳細 セクションで次の手順を実行します。
    1. ブリッジの 名前 を入力します。
    2. ブリッジタイプ として エグレスブリッジ を選択します。
    3. ブリッジ経由で転送するコンテンツの最大ビットレート を入力します。
5. 次に、ソース セクションで以下の手順を実行します。
    1. ソースの 名前 を入力します。エグレスブリッジの場合、ソースは既存の MediaConnect フローから取得され、施設に配信されます。
    2. ネットワーク を選択します。これはゲートウェイのセットアッププロセス中に作成したネットワークです。
    3. フロー ARN を選択します。これは、ソースとして使用する MediaConnect フローの ARN です。
    4. このフローが VPC インターフェース を使用する場合は、それを選択します。
6. 複数のソースを追加する場合は、フェイルオーバー設定 セクションでフェイルオーバーを設定できます。
    a. エグレスブリッジを選択した場合、使用できる フェイルオーバーモード は フェイルオーバー だけです。マージ は選択できません。
    b. ステップ 5 で設定したソースの 1 つを プライマリソース として選択します。
7. エグレスブリッジ作成の最後のセクションは 出力 です。以下の手順を実行します。
    1. 出力グループの 名前 を入力します。
    2. ネットワーク を選択します。これはゲートウェイのセットアッププロセス中に作成したネットワークです。

3. 出力に使用するトランスポート プロトコル を選択します。
4. 出力の IP アドレス を入力します。これはローカルネットワークと互換性のある IP でなければなりません。
5. 出力の ポート を入力します。これはローカルネットワークと互換性のあるポートでなければなりません。
6. 出力の TTL (生存時間) を入力します。

8. ブリッジの作成 を選択します。
9. ブリッジが作成されたら、ブリッジの 詳細 ページで 開始 を選択してブリッジを起動できます。

ゲートウェイの作成 (コンソール)

設定はゲートウェイの作成から始まります。これは、MediaConnect コンソールで MediaConnect API または CloudFormation を使用して、プログラムとして行うことができます。MediaConnect Gateway とそのネットワークが作成されたら、その MediaConnect Gateway へのインスタンスの登録と、それらのインスタンスでのブリッジの作成を開始できます。

トピック

- ゲートウェイ (コンソール) の作成
- インスタンスの登録 (コンソール)
- ブリッジの作成 (コンソール)
- ゲートウェイとそのコンポーネントの削除 (コンソール)

ゲートウェイ (コンソール) の作成

最初のステップは、ゲートウェイとネットワークを作成することです。ゲートウェイは、インスタンスとブリッジを論理的にグループ化したものです。各ゲートウェイは、データセンターと AWS クラウド 間の通信にユーザー定義の IP 情報を活用します。

ゲートウェイを作成するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、ゲートウェイの作成 を選択します。

3. ゲートウェイの作成 ページで、ゲートウェイの 名前 を入力します。この名前は後で変更できません。
4. エグレス CIDR ブロック の場合：ゲートウェイのエグレス側の CIDR ブロックを入力します。IP アドレスを Classless Inter-Domain Routing (CIDR) ブロック (10.0.0.0/16 など) としてフォーマットします。この CIDR ブロックは、コンテンツを提供したり、このゲートウェイと通信するフローの出力リクエストを開始したりできる IP アドレスの範囲を表します。

   > **Important**
   >
   > エグレス CIDR ブロック には 0.0.0.0/0 を使用しないでください。これにより、ゲートウェイが公開されます。

5. ネットワーク セクションに、最初のネットワークの名前を入力します。ゲートウェイには、最大 2 つのネットワークを含めることができます。各ネットワーク名は、このゲートウェイに対して一意である必要があります。
6. このネットワークの CIDR ブロック を入力します。ゲートウェイの作成を完了するには、ゲートウェイの作成 ボタンを選択します。

インスタンスの登録 (コンソール)

ゲートウェイを作成したら、そのゲートウェイにインスタンスを登録できます。インスタンスは、データセンター内の機器上で実行され、MediaConnect によって管理されるコンピューティングリソースです。このインスタンスは MediaConnect サービスのオンプレミス実装であり、ゲートウェイ内に含まれています。インスタンスはブリッジを使用してデータセンターと AWS クラウドの間で通信します。インスタンスは、オンプレミスサーバーにソフトウェアをインストールすることによって作成されます。

インスタンスを登録するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、インスタンスを登録するゲートウェイを選択します。
3. ゲートウェイ 詳細 ページで、インスタンス タブを選択します。
4. インスタンス タブでインスタンスの登録 を選択します。
5. ゲートウェイインスタンスの登録 ページで、次のステップを完了します。

1. アクティベーションキーの期間 を使用する場合、アクティベーションキーがアクティブなままになる日数を入力します。その日数が経過すると、ゲートウェイのインスタンスを登録する際にキーは機能しなくなります。
2. インスタンス数 を使用する場合　アクティベーションキーを使用してクラスターに登録する外部インスタンスの数を入力します。
3. インスタンスロール では、外部インスタンスに関連付ける AWS Identity and Access Management (IAM) ロールを選択します。
4. 登録コマンドの生成 を選択します。

6. Linux コマンド が表示されます。COPY コマンドをコピーします。このコマンドは、このゲートウェイに登録する各インスタンスで実行する必要があります。

> **Important**
>
> スクリプトの bash 部分は root として実行する必要があります。コマンドが root として実行されない場合、エラーが返されます。

7. 数分後、インスタンスはゲートウェイに登録されます。このゲートウェイに登録されているすべてのインスタンスがインスタンス タブに表示されます。

ブリッジの作成 (コンソール)

少なくとも 1 つのインスタンスをゲートウェイに登録したら、ブリッジを作成できます。ブリッジを作成するプロセスは、選択したブリッジタイプによって異なります。

イングレスブリッジを作成するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、ブリッジを作成するゲートウェイを選択します。
3. ゲートウェイの 詳細ページ から、ブリッジ タブを選択します。
4. ブリッジ タブから ブリッジの作成 を選択します。
5. ブリッジの作成 ページの 詳細 セクションで次の手順を実行します。
   1. ブリッジの 名前 を入力します。
   2. イングレスブリッジ のブリッジタイプ を選択します。

3. ブリッジ経由で転送するコンテンツの最大ビットレート を入力します。
4. ブリッジの 最大出力 を入力します。

6. 次に、ソース セクションで以下の手順を実行します。イングレスブリッジのソースは、施設で送信されるマルチキャストコンテンツです。

   1. ソースの 名前 を入力します。
   2. ネットワーク を選択します。これはゲートウェイのセットアッププロセス中に作成したネットワークです。
   3. このソースの プロトコル を選択します。
   4. ソースの マルチキャスト IP と ポート を入力します。

7. 複数のソースを追加する場合、フェイルオーバー設定 セクションを使用してフェイルオーバーを設定できます。

   a. フェイルオーバーモード としてフェイルオーバー またはマージ を選択する
   b. オプション - モードとして フェイルオーバー を選択した場合は、以前に プライマリソース として設定したソースの 1 つを選択できます。プライマリソース を選択しない場合、MediaConnect はランダムに 1 つを選択します。

8. ブリッジの作成を完了するには、ブリッジの作成 を選択します。
9. ブリッジが作成されたら、ブリッジの 詳細 ページで 開始 を選択してブリッジを起動できます。

エグレスブリッジを作成するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、ブリッジを作成するゲートウェイを選択します。
3. ゲートウェイの 詳細 ページで、ブリッジ タブを選択します。ブリッジの作成 を選択します。
4. ブリッジの作成 ページの詳細 セクションで次の手順を実行します。

   1. ブリッジの 名前 を入力します。
   2. エグレスブリッジ の ブリッジタイプ を選択します。
   3. ブリッジ経由で転送するコンテンツの最大ビットレート を入力します。

5. 次に、ソース セクションで以下の手順を実行します。

1. ソースの 名前 を入力します。エグレスブリッジの場合、ソースは既存の MediaConnect フローから取得され、施設に配信されます。
2. ネットワーク を選択します。これはゲートウェイのセットアッププロセス中に作成したネットワークです。
3. フロー ARN を選択します。これは、ソースとして使用する MediaConnect フローの ARN です。
4. このフローが VPC インターフェース を使用する場合は、それを選択します。

6. 複数のソースを追加する場合、フェイルオーバー設定 セクションを使用してフェイルオーバーを設定できます。

   a. エグレスブリッジを選択した場合、使用できる フェイルオーバーモード は [Failover] (フェイルオーバー) だけです。マージ は選択できません。

   b. オプション - 以前に作成したソースの 1 つを プライマリソース として選択します。プライマリソース を選択しない場合、MediaConnect はランダムに 1 つを選択します。

7. エグレスブリッジ作成の最後のセクションは 出力 です。以下の手順を実行します。

   1. 出力グループの 名前 を入力します。
   2. ネットワーク を選択します。これは MediaConnect Gateway のセットアッププロセス中に作成したネットワークです。
   3. 出力するトランスポート プロトコル を選択します。
   4. 出力の IP アドレス を入力します。これはローカルネットワークと互換性のある IP でなければなりません。
   5. 出力の ポート を入力します。これはローカルネットワークと互換性のあるポートでなければなりません。
   6. 出力の生存時間 を入力します。

8. ブリッジの作成 を選択します。
9. ブリッジが作成されたら、ブリッジの詳細ページで 開始 を選択してブリッジを起動できます。

ゲートウェイとそのコンポーネントの削除 (コンソール)

ゲートウェイを削除するには、まずネットワーク、インスタンス、ブリッジなどのコンポーネントをすべて削除する必要があります。ゲートウェイとそのコンポーネントを削除する手順は次のとおりです。

ゲートウェイを削除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで ゲートウェイ を選択します。ゲートウェイ セクションで、削除するゲートウェイを選択します。
3. MediaConnect Gateway の詳細ページで、ブリッジ タブを選択します。ブリッジを削除するには、次のステップを実行します。
   1. 削除するブリッジを選択します。
   2. ブリッジが起動している場合は、停止 を選択します。
   3. ブリッジが停止したら、削除 を選択します。
   4. ブリッジの削除 を選択してブリッジの削除を確定します。
   5. 削除する必要のあるその他のブリッジでも、この手順を繰り返します。
4. ゲートウェイの 詳細 ページに戻り、インスタンス タブを選択します。インスタンスを削除するには、次のステップを実行します。
   1. 削除するインスタンスを選択します。
   2. 登録解除 を選択します。
   3. インスタンスの登録解除 を選択してインスタンスの登録解除を確定します。
   4. 登録解除が必要な追加のインスタンスに対して、これらのステップを繰り返します。

   > **Note**
   >
   > オプション：インスタンスを Amazon ECS Anywhere または別のゲートウェイのインスタンスとして再利用する場合は、次のステップを完了する必要があります。そうでない場合は、ステップ 5 に進みます。

   a. 再利用するインスタンスのインスタンスのステータス が登録解除 になっていることを確認します。
   b. アクセス権を持つコンピューターから、SSH を使用してインスタンスに接続します。
   c. 次の各コマンドを順番に実行します。

```
sudo docker stop $(sudo docker ps -f "name=MediaConnectGatewayAgent" -q); \
sudo docker stop ecs-agent; \
sudo systemctl stop ecs amazon-ssm-agent; \
sudo yum remove -y amazon-ecs-init amazon-ssm-agent;  `# or apt or snap as
 needed` \
sudo rm /var/lib/ecs /etc/ecs /var/lib/amazon/ssm /var/log/ecs /var/log/amazon/
ssm -rf; \
sudo docker rm -f ecs-agent ssm-agent; \
sudo docker container rm -f $(sudo docker ps -a -f
 "name=MediaConnectGatewayAgent" -q); \
sudo docker volume rm -f ecsdata docker run; \
sudo pkill -f -KILL network_bootstra[p]; \
sudo pkill -KILL mcproxy;
```

5. すべてのブリッジを正常に削除し、ゲートウェイに関連付けられているすべてのインスタンスを登録解除したら、ゲートウェイを削除できます。ゲートウェイを削除すると、そのゲートウェイの下に作成されたネットワークもすべて削除されます。

   1. ナビゲーションペインで ゲートウェイ を選択します。
   2. ゲートウェイ セクションで、削除するゲートウェイを選択すると、そのゲートウェイの 詳細 ページが表示されます。
   3. 削除 ボタンを選択します。
   4. ゲートウェイの削除 を選択して、ゲートウェイの削除を確認します。

ゲートウェイの作成 (AWS CLI)

AWS CLI を使用してゲートウェイを作成するには、以下の手順を参照してください。

トピック

ゲートウェイの作成 (AWS CLI)

ゲートウェイは、インスタンスとブリッジを論理的にグループ化したものです。各ゲートウェイは、データセンターと AWS クラウド 間の通信にユーザー定義の IP 情報を活用します。

AWS CLI を使用してゲートウェイを作成する前に、作成するゲートウェイの名前、エグレス CIDR IP 情報、およびネットワーク情報が必要です。この情報は、AWS CLI を実行するコンピュータの JSON ファイルに保存します。JSON ファイルには、gateway.json という名前を付ける必要があります。次の例は、JSON ファイルの正しいセクションと形式を示しています。

```
{
    "Name": "gateway",
    "EgressCidrBlocks": [
        "10.20.30.0/24"
    ],
    "Networks": [
        {
            "Name": "blue",
            "CidrBlock": "172.31.48.0/20",
        }
    ]
}
```

AWS CLI を使用して ゲートウェイを作成するには

1. 次のコマンドを AWS CLI インターフェイスに入力します。<yourprofile> および <region> の値を目的のプロファイルと AWS リージョン に置き換えます。

   ```
   aws --profile <yourprofile> --region <region> mediaconnect create-gateway
         --cli-input-json file://gateway.json
   ```

2. AWS CLI コマンドでは次のようなレスポンスが返されます。

   ```
       "Gateway": {
           "EgressCidrBlocks": [
               "10.20.30.0/24"
           ],
           "GatewayArn": "arn:aws:mediaconnect:us-
   west-2:111122223333:gateway:1-23aBC45dEF67hiJ8-12AbC34DE5fG:gateway",
           "GatewayState": "CREATING",
           "Name": "gateway",
           "Networks": [
               {
                   "CidrBlock": "172.31.48.0/20",
                   "Name": "blue"
               }
           ]
   ```

```
    }
}
```

3. MediaConnect Gateway が作成されました。

インスタンスの登録 (AWS CLI)

ゲートウェイを作成したら、そのゲートウェイにインスタンスを登録できます。インスタンスは、データセンター内の機器上で実行され、MediaConnect によって管理されるコンピューティングリソースです。このインスタンスは MediaConnect サービスのオンプレミス実装であり、ゲートウェイ内に含まれています。インスタンスはブリッジを使用してデータセンターと AWS クラウド の間で通信します。インスタンスは、オンプレミスサーバーにソフトウェアをインストールすることによって作成されます。

AWS CLI を使用したインスタンスの登録は、現在サポートされていません。インスタンスの登録 (コンソール) のコンソールの指示に従い、AWS コンソールを使用してインスタンスを登録します。

ブリッジの作成 (AWS CLI)

少なくとも 1 つのインスタンスをゲートウェイコンポーネントに登録したら、ブリッジを作成できます。ブリッジはインスタンスと AWS クラウド をつなぐものです。

AWS CLI を使用してブリッジを作成する前に、作成するブリッジの詳細を収集する必要があります。これらの詳細は、AWS CLI を実行しているコンピュータの JSON ファイルに保存されます。JSON ファイルには、`bridge.json` という名前を付ける必要があります。次の例は、JSON ファイルの正しいセクションと形式を示しています。

```
{
    "Name": "bridge",
    "PlacementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:gateway:1-23aBC45dEF67hiJ8-12AbC34DE5fG:gateway",
    "EgressGatewayBridge": {
        "MaxBitrate": 100000000
    },
    "SourceFailoverConfig": {
        "FailoverMode": "FAILOVER",
        "State": "ACTIVE"
    },
    "Sources": [
        {
            "FlowSource": {
                "Name": "Source0",
                "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
UAECXlABCQJeVwMB-95ec11ac6059:gatewayFlow",
                "NetworkName": "blue"
            }
        },
        {
            "FlowSource": {
                "Name": "Source1",
                "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
ECRZVGADYMGtPGTM-c1iPQ5FNL7Qn:gatewayFlow",
                "NetworkName": "blue",
                "FlowVpcInterfaceAttachment": {
                    "VpcInterfaceName": "VPCIF"
                }
            }
        }
    ],
    "Outputs": [
        {
            "NetworkOutput": {
                "Name": "Output0",
                "NetworkName": "blue",
                "IpAddress": "225.1.2.3",
                "Port": 5010,
                "Protocol": "rtp-fec",
                "Ttl": 8
            }
        },
```

```
        {
            "NetworkOutput": {
                "Name": "Output1",
                "NetworkName": "blue",
                "IpAddress": "225.1.2.4",
                "Port": 6010,
                "Protocol": "rtp",
                "Ttl": 250
            }
        }
    ]
}
```

AWS CLI を使用してブリッジを作成するには

1. 次のコマンドを AWS CLI インターフェイスに入力します。<yourprofile> および <region> の値を目的のプロファイルと AWS リージョン に置き換えます。

```
aws --profile <yourprofile> --region <region> mediaconnect create-bridge
      --cli-input-json file://bridge.json
```

2. AWS CLI コマンドでは次のようなレスポンスが返されます。

```
{
    "Bridge": {
        "BridgeArn": "arn:aws:mediaconnect:us-west-2:111122223333:bridge:1-
GLxlBRLrHzzvpwyb-1dd820
66b207:bridge",
        "BridgeMessages": [],
        "BridgeState": "STANDBY",
        "EgressGatewayBridge": {
            "MaxBitrate": 100000000
        },
        "Name": "bridge",
        "Outputs": [
            {
                "NetworkOutput": {
                    "IpAddress": "225.1.2.3",
                    "Name": "Output0",
                    "NetworkName": "blue",
                    "Port": 5010,
                    "Protocol": "rtp-fec",
                    "Ttl": 8
                }
            },
            {
                "NetworkOutput": {
                    "IpAddress": "225.1.2.4",
                    "Name": "Output1",
                    "NetworkName": "blue",
                    "Port": 6010,
                    "Protocol": "rtp",
                    "Ttl": 250
                }
            }
        ],
        "PlacementArn": "arn:aws:mediaconnect:us-
west-2:111122223333:gateway:1-23aBC45dEF67hiJ8-12AbC34DE5fG:gateway",
        "SourceFailoverConfig": {
            "FailoverMode": "FAILOVER",
            "State": "ENABLED"
        },
        "Sources": [
            {
                "FlowSource": {
                    "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
UAECXlABCQJeVwMB-95ec11ac6059:gatewayFlow",
```

```
                    "Name": "Source0",
                    "NetworkName": "blue"
                }
            },
            {
                "FlowSource": {
                    "FlowArn": "arn:aws:mediaconnect:us-west-2:111122223333:flow:1-
ECRZVGADYMGtPGTM-c1iPQ5FNL7Qn:gatewayFlow",
                    "Name": "Source1",
                    "NetworkName": "blue",
                    "FlowVpcInterfaceAttachment": {
                        "VpcInterfaceName": "VPCIF"
                    }
                }
            }
        ]
    }
}
```

3. ブリッジが作成されました。

ゲートウェイとそのコンポーネントの削除 (AWS CLI)

ゲートウェイを削除するには、まずネットワーク、インスタンス、ブリッジなどのコンポーネントをすべて削除する必要があります。AWS Command Line Interface (AWS CLI) を使用してゲートウェイとそのコンポーネントを削除するプロセスを以下に示します。

AWS CLI を使用してゲートウェイを削除するには

1. 次のコマンドを実行して、ブリッジを削除します。

```
aws --profile <Profile> --region <Region> mediaconnect delete-bridge --bridge-
arn <BridgeArn>
```

2. 次のコマンドを実行して、インスタンスを登録解除します。

```
aws --profile <Profile> --region <Region> mediaconnect deregister-gateway-instance
 --gateway-instance-arn <GatewayArn>
```

> **Note**
>
> オプション：インスタンスを Amazon ECS Anywhere または別のAWS Elemental MediaConnect Gatewayのインスタンスとして再利用する場合は、次のステップを完了する必要があります。そうでない場合は、ステップ 3 に進みます。

a. 再利用するインスタンスの InstanceState が DEREGISTERED であることを確認してください。次の例に示す describe-gateway-instance コマンドを使用して確認できます。

```
aws --profile <Profile> --region <Region> mediaconnect describe-gateway-
instance
      --gateway-instance-arn <GatewayInstanceArn>
```

b. アクセス権を持つコンピューターから、SSH を使用してインスタンスに接続します。

c. 次の各コマンドを順番に実行します。

```
sudo docker stop $(sudo docker ps -f "name=MediaConnectGatewayAgent" -q); \
sudo docker stop ecs-agent; \
sudo systemctl stop ecs amazon-ssm-agent; \
sudo yum remove -y amazon-ecs-init amazon-ssm-agent;  `# or apt or snap as
 needed` \
sudo rm /var/lib/ecs /etc/ecs /var/lib/amazon/ssm /var/log/ecs /var/log/amazon/
ssm -rf; \
sudo docker rm -f ecs-agent ssm-agent; \
sudo docker container rm -f $(sudo docker ps -a -f
 "name=MediaConnectGatewayAgent" -q); \
sudo docker volume rm -f ecsdata docker run; \
sudo pkill -f -KILL network_bootstra[p]; \
sudo pkill -KILL mcproxy;
```

3. ゲートウェイを削除します。これにより、ゲートウェイに関連するすべてのネットワークが削除されます。

```
aws --profile <Profile> --region <Region> mediaconnect delete-gateway --gateway-
arn <GatewayArn>
```

VPC インターフェイス

Amazon Virtual Private Cloud サービスに基づく Virtual Private Cloud (VPC) は、 AWS クラウド内の論理的に分離されたプライベートネットワークです。VPC インターフェイスを設定して、AWS Elemental MediaConnect フローと VPC 間の接続を確立できます。

詳細については、次のセクションを参照してください。

- VPC ソースを使用するトランスポートストリームフローの作成
- MediaConnect フローへの VPC インターフェイスの追加
- MediaConnect フローからの VPC インターフェイスの削除
- VPC ソースを既存のフローに追加します
- VPC 出力をフローに追加する
- VPC インターフェイスのセキュリティグループに関する考慮事項

MediaConnect フローへの VPC インターフェイスの追加

パブリックインターネット経由でコンテンツをストリーミングしないようにするには、AWS Elemental MediaConnect フローに VPC インターフェイスを追加できます。各フローには、最大 2 つの VPC インターフェイスを追加できます。

> **Important**
>
> VPC インターフェイスを追加すると、MediaConnect は にサービスマネージド Elastic Network Interface (ENI) を作成します AWS アカウント。適切なサービスオペレーションを確保するために、このリソースはいかなる方法でも変更しないでください。

前提条件

この手順を開始する前に、次のステップを完了していることを確認してください。

- Amazon VPC で、VPC と関連するセキュリティグループを設定します。VPC の詳細については、「Amazon VPC ユーザーガイド」を参照してください。VPC インターフェイスと連携するようにセキュリティグループを設定する方法については、「セキュリティグループに関する考慮事項」を参照してください。

- IAM で、MediaConnect を信頼されたサービスとしてセットアップします。

手順

VPC インターフェイスをフロー (コンソール) に追加するには

1. フローページで、更新するフローの名前を選択します。
2. [VPC インターフェイス] タブを選択します。
3. [VPC インターフェイスを追加] を選択します。
4. [名前] には、VPC インターフェイスの名前を指定します。VPC インターフェイスの名前は、フロー内で一意である必要があります。
5. ネットワークインターフェイスタイプ には、MediaConnect にこのインターフェースで使用させたいネットワークアダプターのタイプを指定します。この値を指定していない場合は、デフォルトで ENA になります。

   > **Note**
   >
   > - フローごとに 1 つの EFA VPC インターフェイスを追加できます。
   > - フローごとに最大 2 つの ENA VPC インターフェイスを追加できます。
   > - EFA VPC インターフェイスは、CDI プロトコルまたは ST 2110 と JPEG XS プロトコルを使用するソースにのみ使用できます。

6. ロール ARN では、MediaConnect を信頼できるサービスとして設定したときに作成したロールの Amazon リソースネーム (ARN) を指定します。
7. [VPC] では、使用する VPC の ID を選択します。
8. [サブネット] では、MediaConnect が VPC 設定のセットアップに使用する VPC サブネットを選択します。サブネットはフローと同じアベイラビリティーゾーンに存在する必要があります。
9. [セキュリティグループ] では、MediaConnect が VPC 設定のセットアップに使用する VPC セキュリティグループを指定します。少なくとも 1 つのセキュリティグループを選択する必要があります。

その他のリソース

VPC フローログを使用して、VPC 内のネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報をキャプチャできます。フローログデータは、CloudWatch Logs、Amazon S3、または Data Firehose に発行できます。VPC フローログの詳細については、「Amazon VPC ユーザーガイド」の「VPC フローログを使用した IP トラフィックのログ記録」を参照してください。

MediaConnect フローからの VPC インターフェイスの削除

VPC インターフェイスがフローのソースとして使用されていない場合は、フローから削除できます。

前提条件

- フローはスタンバイになっている必要があります。
- フローにエラーがある場合は、次の手順を完了する前にエラーを解決する必要があります。

手順

VPC インターフェイスをフロー (コンソール) から 削除するには

1. フロー ページで、削除する VPC インターフェイスに関連付けられたフローの名前を選択します。
2. [停止] を選択します。

   DB インスタンスのステータスが [スタンバイ] に変更されます。フローはすぐに停止し、フローから直接出力にアクセスしたり、使用権限を通じて出力にアクセスしたりする顧客が見ることはできなくなります。
3. [VPC インターフェイス] タブを選択します。
4. 削除する VPC インターフェイスを選択し、削除する を選択します。

VPC インターフェイスのセキュリティグループに関する考慮事項

Amazon Virtual Private Cloud で仮想プライベートクラウド (VPC) を設定すると、インバウンドトラフィックとアウトバウンドトラフィックを制御するセキュリティグループを作成します。次

に、AWS Elemental MediaConnect で VPC インターフェイスを作成するときに、MediaConnect が VPC からコンテンツを送受信するときに使用するセキュリティグループを指定します。

VPC と MediaConnect の間でコンテンツが流れるようにするには、次のガイドラインに従ってください。

VPC インターフェイスに、以下を有するセキュリティグループがあることを確認してください	追加情報
コンテンツを送信している VPC 内のリソースのプライベート IP アドレスを許可するインバウンドルール。	Zixi ソース: Zixi プロトコルを使用して VPC ソースを作成すると、受信ポートは MediaConnect によって自動的に割り当てられます。割り当てられるポートは 2090 ~ 2099 の範囲で、ソース作成時に割り当てられます。最初に Zixi VPC ソースを作成し、割り当てられたポートを書き留めておく必要があります。ポート情報を割り当てたら、セキュリティグループを設定できます。
すべてのアウトバウンドトラフィックを許可するアウトバウンドルール。デフォルトでは、すべてのセキュリティグループにこのルールが含まれます。セキュリティグループからルールを削除しない限り、新しく作成する必要はありません。	フローからトラフィックを受信するリソースでは、VPC インターフェイスに関連付けられているネットワークインターフェイス ID のプライベート IP を許可するインバウンドルールを使用して、セキュリティグループも設定する必要があります。(MediaConnect では、フローの詳細を確認してネットワークインターフェイス ID を確認できます。 次に EC2 では、ネットワークインターフェイスに関する詳細を表示して IP アドレスを取得します。)
上記の要件を満たすインバウンドルールとアウトバウンドルール。	両方のルールを含む 1 つのセキュリティグループを使用することも、2 つのセキュリティグループ (各ルールに 1 つずつ) を使用することもできます。 CDI フローの場合、VPC インターフェイスに指定されたセキュリティグループは自己参照である必要があります。使用するセキュリティグループに、インバウンドルールとアウトバウンドルール

VPC インターフェイスに、以下を有するセキュリティグループがあることを確認してください	追加情報
	の両方に同じセキュリティグループ ID が追加されていることを確認します。

詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループ」を参照してください。

AWS Elemental MediaConnect におけるメディアストリーム

メディアストリームは CDI フローに欠かせないコンポーネントです。メディアストリームを使用し、SMPTE 2110 (パート 22 トランスポート標準) を介してコンテンツを AWS クラウドに取り込み、クラウド内で転送できます。各メディアストリームは、動画、オーディオ、または補助データを含む 1 つのメディアトラックまたはメディアストリームを表します。

メディアストリームはフローの一部として定義します。次に、そのフローの 1 つのソースと複数の出力に関連付けることができます。ソースと出力は CDI プロトコルまたは ST 2110 JPEG XS プロトコルを使用する必要があり、1 つまたは複数のメディアストリームで構成できます。

作成するメディアストリームのタイプは、AWS Elemental Live などのオンプレミスデバイスとの間で送受信する出力に基づいています。

> **Note**
>
> メディアストリームは、入出力プロトコルとして ST 2110 と JPEG XS を使用する CDI フローにのみ使用します。CDI を入力および出力プロトコルとして使用するようにフローを構成している場合、メディアストリームは必要ありません。

AWS Elemental Live (出力)	MediaConnect メディアストリームタイプ
SMPTE 2110-20: 非圧縮動画	(サポート外)
SMPTE 2110-22: JPEG XS による圧縮動画	動画
SMPTE 2110-30: PCM オーディオ	オーディオ
SMPTE 2110-31: Dolby オーディオ (AC3、EAC3)	(サポート外)
SMPTE 2110-40: 補助データ	補助データ

CDI ワークフローの図については、CDI フローへのコントリビューション と CDI のレプリケーションとモニタリング を参照してください。

トピック

メディアストリームをフローに追加する

メディアストリームをソースまたは出力に関連付ける前に、フローに追加する必要があります。メディアストリームをフローに追加したら、まずソースに関連付けてから、その後出力に関連付けることができます。

> **Note**
>
> メディアストリームを出力に関連付けることができるのは、フロー上でそのメディアストリームがソースにすでに関連付けられている場合だけです。

メディアストリームをフローに追加するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、メディアストリームを追加するフローの名前を選択します。
3. メディアストリーム タブを選択します。
4. メディアストリームを追加 を選択します。
5. 名前 フィールドに、このメディアストリームをフロー内の他のメディアストリームと区別するのに役立つわかりやすい名前を指定します。
6. 説明 には、このメディアストリームの使用を覚えやすい説明を指定します。
7. ストリーム ID には、メディアストリームの固有識別子を指定します。

   ソースまたはいずれかの出力が CDI プロトコルを使用している場合は、プロダクションシステムやプレイアウトシステムで想定される値を指定します。

   ソースとすべての出力が ST 2110 JPEG XS プロトコルを使用している場合は、フロー内の他のメディアストリームに固有の値を指定してください。
8. 詳細オプション を選択すると、ストリームのタイプに基づいて追加オプションが表示されます。
9. ストリームのタイプに応じた詳細オプションの具体的な手順については、以下のタブのいずれかを選択してください。

Audio

1. ストリームタイプ には オーディオ を選択します。
2. メディアクロックレート には、ストリームのサンプルレートを指定します。この値は Hz 単位で測定されます。
3. 言語 には、オーディオの言語を指定します。この値は、レシーバーが認識できる形式である必要があります。
4. チャンネルオーダー では、オーディオチャンネルの形式を指定します。
5. メディアストリームを追加 を選択します。

Video

1. ストリームタイプ には 動画 を選択します。

   多くのフィールドでは、MediaConnect は推奨設定を表すデフォルト値を提供します。必要に応じてデフォルト値を変更してください。
2. メディアクロックレート はストリームのサンプルレートであり、90000 に設定されています。この値は Hz 単位で測定されます。
3. 動画形式 では、動画の解像度を指定します。
4. 正確なフレームレート では、動画のフレームレートを指定します。この値は 1 秒あたりのフレーム数で表す必要があります。
5. 色度測定 には、動画の色を表現するために使用された形式を指定します。
6. スキャンモード には、受信したビデオをスキャンするために使用された方法を指定します。
   - 受信動画がインターレースされている場合 (480i や 1080i など) は、インターレース を選択します。
   - 受信ビデオがプログレッシブ (720p や 1080p など) の場合は、プログレッシブ を選択します。
   - 受信ビデオが PSF (1080psf など) の場合は、プログレッシブセグメントフレーム を選択します。
7. TCS には、ビデオで使用されていた伝達特性システム (TCS) を指定します。
8. 範囲 には、ビデオのエンコード範囲を指定します。
9. PAR には、動画のピクセルアクセス率 (PAR) を指定します。

10.メディアストリームを追加 を選択します。

Ancillary data

1. ストリームタイプ には、補助データ を選択します。
2. メディアクロックレート はストリームのサンプルレートであり、90000 に設定されています。この値は Hz 単位で測定されます。
3. メディアストリームを追加 を選択します。

メディアストリームの更新

メディアストリームは、フローが実行中でも更新できます。ただし、メディアストリームがソースまたはいずれかの出力に関連付けられている場合は、そのタイプを更新できません。

フロー上のメディアストリームを更新するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、更新するメディアストリームに関連するフローの名前を選択します。
3. メディアストリーム タブを選択します。

   そのフローのメディアストリームのリストが表示されます。
4. 更新するメディアストリームを選択します。
5. [Update] (更新) を選択します。
6. 適切な変更を行い、[Save] (保存) を選択します。

メディアストリームの削除

フローがアクティブでなく、メディアストリームがソースや出力に関連付けられていない場合は、フローからメディアストリームを削除できます。

メディアストリームをフローから削除するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. フロー ページで、削除するメディアストリームに関連するフローの名前を選択します。

   そのフローの詳細ページが表示されます。

3. メディアストリーム タブを選択します。
4. メディアストリームを選択し、削除 を選択します。

AWS Elemental MediaConnect の予約

オンデマンド料金と比較して、予約することで AWS Elemental MediaConnect の料金を大幅に節約することができます。

予約とは、指定された期間にわたって、毎月特定の量のアウトバウンド帯域幅を使用することを約束することです。その代わりに、その帯域幅に対して割引された時間料金を支払います。予約は予約期間中、月単位で割り当てられ、請求されます。

割引料金は、予約で指定された帯域幅を上限として、アカウント内のすべての MediaConnect フローからのアウトバウンド帯域幅に適用されます。

アウトバウンド帯域幅とは、MediaConnect フローから AWS クラウド外の場所またはエンドポイントに転送されるデータを指します。これには、MediaConnect フローに転送されたデータや、MediaConnect フローから AWS クラウド内の任意の場所に転送されたデータは含まれません。

予約の料金に関する詳細については、MediaConnect の料金表 を参照してください。

請求の仕組み

予約済みのアウトバウンド帯域幅は 1 時間ごとに請求されます。請求サイクルごとに、AWS は、予約時に指定された割引料金で、アウトバウンド帯域幅の料金をアカウントに請求します。アカウントが予約でカバーされているよりも多くのアウトバウンド帯域幅を使用している場合、超過分はオンデマンド料金で請求されます。アカウントが使用した帯域幅が少ない場合、AWS は予約で指定されたアウトバウンド帯域幅の量に対して料金を請求します。未使用の帯域幅は翌月に繰り越されません。

予約の表示

コンソールで、購入した予約を表示できます。

予約の一覧を表示するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで、[Reservations] (予約) を選択します。

   購入したすべての予約を示すリストが表示されます。

サービス

サービスとは、MediaConnect が毎月一定量のアウトバウンド帯域幅を使用するという約束と引き換えに提供される割引です。MediaConnect サービスの構成要素は以下のとおりです。

- [Duration] (所要時間)
- アウトバウンド帯域幅
- 料金 (時間単位で請求)

サービスを購入する際は、開始日と時間を指定します。生成されるリソースは予約と呼ばれます。これは、一定量のアウトバウンド帯域幅を一定期間に「予約」することになるからです。

アウトバウンド帯域幅とは、MediaConnect フローから AWS クラウド外の場所またはエンドポイントに転送されるデータを指します。これには、MediaConnect フローに転送されたデータや、MediaConnect フローから AWS クラウド内の任意の場所に転送されたデータは含まれません。

サービスの表示

コンソールでは、現在の AWS リージョンで利用できるサービスを表示できます。

サービスの一覧を表示するには (コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで、サービス を選択します。

   現在のリージョンで利用できるすべてのサービスを示すリストが表示されます。

サービスの購入

アカウントにまだ有効な予約がない場合は、サービスを購入して新しい予約を作成できます。

サービスを購入するには(コンソール)

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで、サービス を選択します。

   現在のリージョンで利用できるすべてのサービスを示すリストが表示されます。

> **Note**
>
> 有効な予約がある場合、他のサービスを購入することはできません。

3. 購入する予約を選択して、購入 を選択します。

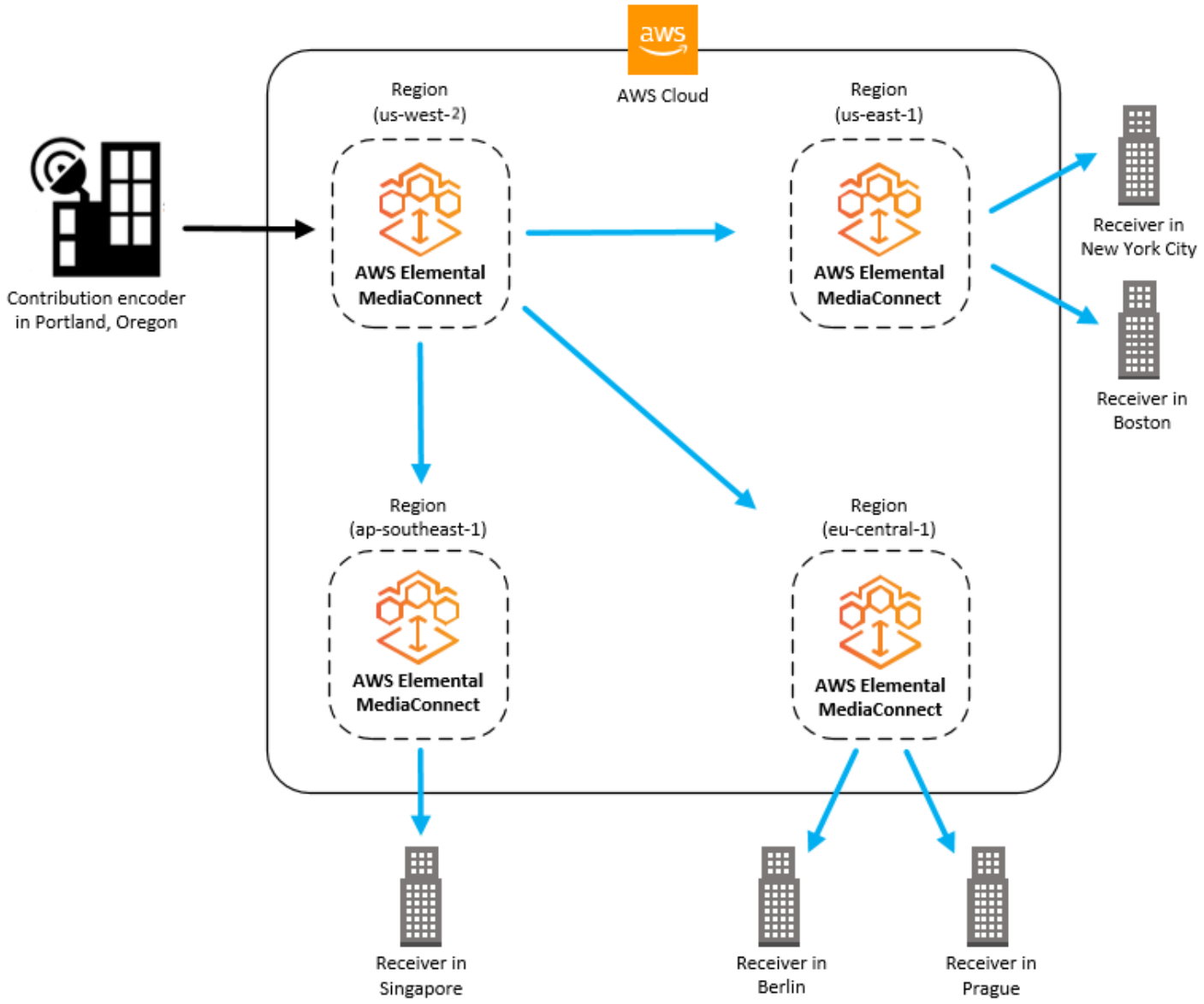
   予約の詳細を入力 ページが表示されます。
4. 名前 フィールドに予約の名前を入力します。予約名は、期限切れの予約も含め、アカウント内で一意である必要があります。
5. 開始日 では、カレンダーアイコンをクリックし、予約を開始する日付を選択します。日付は、早ければ当月の初日から、遅くは今日を選択できます。
6. 開始時刻 フィールドに、予約を開始したい時刻を入力します。開始日が過去の場合は、任意の時刻を選択できます。開始日が今日の場合は、現在時刻までの任意の時刻を選択できます。
7. [Next] (次へ) をクリックします。

   確認と作成 ページが表示されます。
8. 予約の詳細を確認します。予約名または予約名に変更を加える必要がある場合は、前へ を選択して変更を行います。別のサービスを選択する必要がある場合は、キャンセル を選択して最初からやり直してください。
9. [Purchase] (購入) を選択します。

AWS Elemental MediaConnect を使用してコンテンツを配信する

AWS Elemental MediaConnect を使用して、コンテンツをさまざまな地域に配信できます。例えば、ソースがオレゴン州ポートランドにあるオンプレミスのコントリビューションエンコーダーで、世界各地にコンテンツを配信したいとします。最初の AWS Elemental MediaConnect フローは、エンコーダーに最も近い物理us-west-2リージョンである AWS リージョンにセットアップします。コンテンツが AWS クラウドに配置されたら、受信者に近いリージョンにある他の MediaConnect フローに送信します。

次の図は、 AWS クラウド内の AWS Elemental MediaConnect にコンテンツをアップロードするオレゴン州ポートランドにあるオンプレミスのコントリビューションエンコーダーを示しています。フローには、異なる AWS リージョンの他のフローにコンテンツを送信する 3 つの出力があります。これらの 2 次フローは、世界中のさまざまな都市に設置されたレシーバーにより近いフローです。



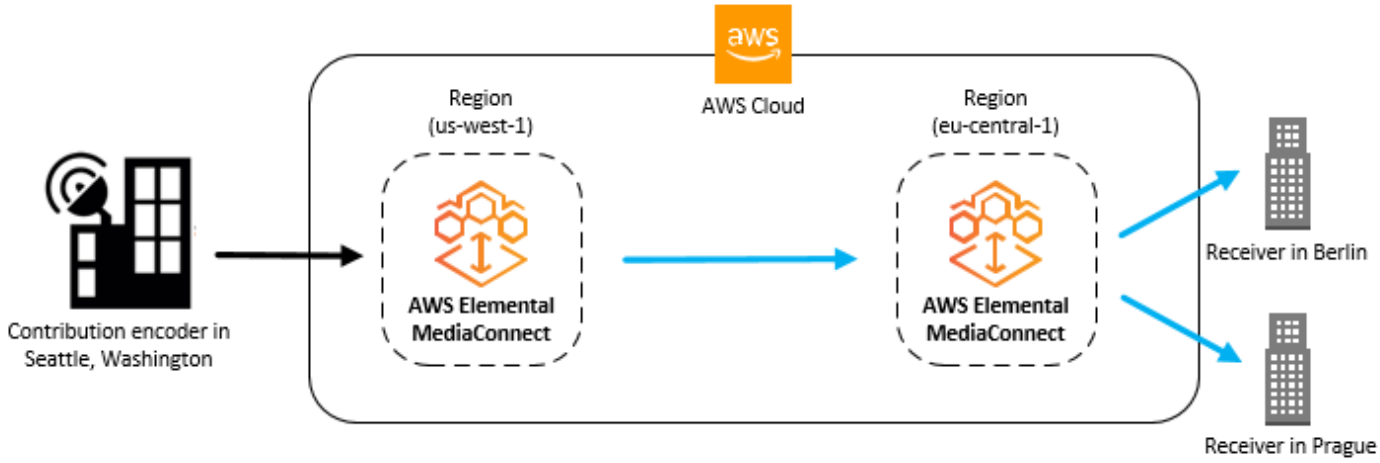
トピック

- リージョン間でのコンテンツの配信
- MediaConnect から MediaLive へのコンテンツの配信
- AWS Elemental MediaLive マルチプレックスからのコンテンツの配信

リージョン間でのコンテンツの配信

2 つの AWS Elemental MediaConnect フローを設定して、あるリージョンから別の AWS リージョンにコンテンツを配信できます。このシナリオでは、コントリビューションエンコーダーに最も近い

リージョンに 1 つのフローを作成し、レシーバーに最も近いリージョンに 2 つ目のフローを作成します。次の図はこのプロセスを示しています。



このトピックは、フローを作成してフローに出力を追加する方法をすでに理解していることを前提としています。

コンテンツを複数のリージョン (コンソール) に配信するには

1. ソースに最も近い AWS リージョンで、フローを作成します。(このフローを A と呼びます)。
2. フロー A の [詳細] ページを確認して、出力 IP アドレスを確認します。
3. 送信先に最も近い AWS リージョンで、次の詳細を含む 2 番目のフロー (フロー B) を作成します。
   - ソースタイプ:[標準ソース] を選択します。
   - プロトコル: [Zixi プッシュ] を選択します。
   - インバウンドポート: プロトコルとして Zixi プッシュ を選択すると、このポートは自動的に **2088** に設定されます。
   - 許可リスト CIDR ブロック: フロー A の出口 IP を含む CIDR 値を入力します。
4. フロー B の [詳細] ページの [ソース] タブを確認して、取り込み IP アドレスを確認します。
5. フロー A で、以下の詳細を含む出力を作成します。
   - プロトコル: [Zixi プッシュ] を選択します。
   - IP アドレス: フロー B の取り込み IP アドレスを入力します。
   - ポート: **2088** を入力します。

MediaConnect から MediaLive へのコンテンツの配信

でフローを設定 AWS Elemental MediaConnect して、コンテンツを配信できます AWS Elemental MediaLive。この設定により、MediaConnect フローは MediaLive チャネルのアップストリーム入力として機能し、MediaLive がビデオストリームを処理できるようになります。

前提条件

開始する前に、以下を確認してください。

- MediaConnect の管理者権限がある
- MediaLive の管理者権限を持つユーザーと調整できます

> **Note**
>
> このページでは、MediaConnect の観点からプロセスについて説明します。 MediaLive 必要なアクセス許可がある場合、1 人のユーザーが両方のロールを実行できます。

手順

- the section called “ステップ 1: MediaLive のアクセス許可を検証する”
- the section called “ステップ 2: MediaLive チャネルの詳細を取得する”
- the section called “ステップ 3. MediaConnect フローを設定する”
- the section called “ステップ 4: MediaLive に接続してフローを開始する”
- the section called “ステップ 5: MediaLive チャネルを開始する”

ステップ 1: MediaLive のアクセス許可を検証する

MediaConnect フローを MediaLive チャネルの入力として使用するには、まず MediaLive がフローを操作するために必要なアクセス許可を持っていることを確認します。これは 1 回限りの設定です。

アクセス許可を確認するには

- MediaLive オペレーターに、MediaLive が MediaConnect フローとやり取りするために必要なアクセス許可が設定されていることを確認します。好みのアプローチを選択できます。

- シンプルなオプション (推奨)

  MediaLive が MediaConnect MediaConnect を操作するために必要なすべてのアクセス許可`MediaLiveAccessRole`を含む を使用します。手順については、「信頼されたエンティティの作成 - シンプルなオプション」を参照してください。

- 複雑なオプション

  より具体的なカスタムアクセス許可が必要な場合は、独自の IAM ポリシーとロールを作成します。または、これらの特定の MediaConnect アクセス許可を既存のカスタム IAM ポリシーとロールに追加することもできます。手順については、「信頼されたエンティティの作成 - 複合オプション」を参照してください。

このステップの結果

MediaLive は、出力の作成と削除、フロー情報の読み取りなど、フローを操作するために必要なアクセス許可を持つようになりました。このロールは、複数のチャネルとフローで再利用できます。

ステップ 2: MediaLive チャネルの詳細を取得する

フローを設定する前に、接続先の MediaLive チャネルに関する特定の情報が必要です。チャネル設定によって、フローに使用する とアベイラビリティーゾーンが決まり AWS リージョン ます。

チャネルの詳細を取得するには

1. MediaLive オペレータと連携して、チャネルに関する情報を取得します。既存のチャネルを使用するか、まだチャネルがない場合は新しいチャネルを作成できます。
2. チャネルに関する以下の情報を提供するよう依頼します。

   - AWS リージョン
   - アベイラビリティーゾーン
   - チャネルタイプ (シングルパイプラインまたはデュアルパイプライン)

このステップの結果

これで、正しい AWS リージョン およびアベイラビリティーゾーンでフローを作成するために必要な情報を取得しました。

ステップ 3. MediaConnect フローを設定する

このステップでは、MediaLive チャネルの入力として機能する新しいフローを作成します (または既存のフローを識別します)。

フローを設定するには

1. MediaConnect コンソールにサインインします。
2. MediaLive チャネルタイプに基づいて、必要なフローの数を決定します。
   - 単一パイプラインチャネルの場合

     チャネルと同じアベイラビリティーゾーンに 1 つのフローが必要です。
   - 標準 (デュアルパイプライン) チャネルの場合

     異なるアベイラビリティーゾーンに 2 つのフローが必要です (2 つの MediaLive チャネルアベイラビリティーゾーンに一致)。
3. 既存のフローを使用するか、新しいフローを作成するかを決定します。
   - 既存のフローを使用している場合

     フローが次の要件を満たしていることを確認します。
     - これらは MediaLive チャネルと同じリージョンにあります。
     - アベイラビリティーゾーンの数と配置が正しい (ステップ 2 で決定)。
     - 十分な帯域幅容量があります。
     - 出力の最大数に達していません。(MediaLive で入力を作成すると、MediaLive は各フローに出力を自動的に作成します)。

     これらの要件が満たされている場合は、ステップ 4 に進みます。それ以外の場合は、新しいフローを作成します。
   - 新しいフローを作成する場合

     MediaLive チャネル AWS リージョン と同じ にフローを作成し、アベイラビリティーゾーンの配置が正しいことを確認します (ステップ 2 で決定)。

> **Tip**
>
> 2 つのフローを作成する場合は、サフィックスを除いて同じ名前を使用します。例えば、**sports_event_A** と **sports_event_B** です。これは、MediaLive オペレーターがフローを MediaLive の入力パイプラインと照合するのに役立ちます。

4. フローの Amazon リソースネーム (ARN) を書き留め、この情報を MediaLive オペレーターと共有します。フロー ARNsようになります。

   - `arn:aws:mediaconnect:us-west-1:111122223333:flow:1bgf67:sports_event_A`
   - `arn:aws:mediaconnect:us-west-1:111122223333:flow:9pmlk76:sports_event_B`

このステップの結果

フローが正しいリージョンとアベイラビリティーゾーンにあり、MediaLive 入力に接続する準備ができています。

ステップ 4: MediaLive に接続してフローを開始する

フローの準備ができたら、詳細を MediaLive に提供して開始できます。

MediaLive に接続してフローを開始するには

1. MediaLive 演算子と調整します。

   - からのフロー ARNs を提供しますthe section called “ステップ 3. MediaConnect フローを設定する”。
   - これらのフロー ARNs を使用して MediaLive チャネルで MediaConnect MediaConnect 入力を作成できるようになりました。

2. MediaConnect で、 で設定した各フローを開始しますthe section called “ステップ 3. MediaConnect フローを設定する”。

> **Note**
>
> MediaLive が入力を作成する前または後にフローを開始できます。順序は関係ありません。MediaLive は、実行中のフローまたはまだ開始されていないフローに出力を追加できます。

このステップの結果

MediaLive は、入力に 2 つのエンドポイントを自動的に作成し (単一パイプラインチャネルでも) 、MediaConnect フローへの接続を確立します。これでフローが実行され、アップストリームソースからコンテンツを受信する準備が整いました。

ステップ 5: MediaLive チャネルを開始する

MediaConnect フローが開始されたら、最後のステップとして MediaLive チャネルを開始します。

MediaLive チャンネルを開始するには

- MediaLive オペレータに、MediaConnect 入力を使用するように設定されたチャネルを開始できることを伝えます。

このステップの結果

MediaLive チャンネルは、フローからのコンテンツの取り込みを開始し、チャンネルの設定に従って処理します。

これでセットアッププロセスが完了します。MediaConnect フローが MediaLive チャネルの入力として機能するようになりました。

請求に関する考慮事項

MediaLive の入力ソースとして MediaConnect を使用する場合は、コストに影響を与える可能性がある以下の考慮事項に注意してください。 MediaLive

MediaLive チャネルを停止した場合の請求への影響

- MediaConnect を入力として使用する MediaLive チャンネルを停止または一時停止しても、関連する MediaConnect 出力も自動的に停止しません。その結果、MediaLive チャネルがア

クティブではなくなった場合でも、MediaConnect 出力はデータの送信を試みます。これにより、MediaConnect フローに追加料金が発生する可能性があります。

追加料金の軽減

- このシナリオで不要な料金が発生しないように、関連する MediaLive チャネルが使用されなくなるたびに MediaConnect フローを手動で停止することをお勧めします。 MediaLive フローを自分で停止することも、MediaLive チームと協力して停止することもできます。
- 別の MediaLive チームを使用する場合は、MediaConnect フローを使用する MediaLive チャネルを一時停止または停止するときに通知することをお勧めします。これにより、これらの期間中に関連する MediaConnect 出力を一時的に停止し、追加料金を回避できます。MediaLive チームと MediaConnect チーム間のこの調整は、サービスのアクティブな使用に対してのみ料金を支払うのに役立ちます。

MediaConnect の使用による料金と請求への影響の詳細については、このガイドの「料金」セクションを参照してください。

AWS Elemental MediaLive マルチプレックスからのコンテンツの配信

マルチ AWS Elemental MediaLive プレックスは、マルチプログラムトランスポートストリーム (MPTS) とも呼ばれる複数のプログラムを伝送する UDP トランスポートストリーム (TS) を作成します。マルチプレックスを作成すると、MediaLive はお客様のアカウントに MediaConnect のエンタイトルメントを自動的に付与します。そのエンタイトルメントに基づいてフローを作成し、そのフローのコンテンツを配信します。

MediaLive マルチプレックス (コンソール) からコンテンツを配信するには

1. MediaLive で、マルチプレックスを作成します。

   MediaLive は、マルチプレックスをソースとして使用する MediaConnect エンタイトルメントを作成します。エンタイトルメントの名前には、`multiplex` およびマルチプレックス用に選択した名前が含まれます。
2. MediaConnect で、新しい使用権限に基づいてフローを作成します。
3. 出力を追加してコンテンツを配信します。

MediaLive からの SRT 出力の受信

SRT プロトコルを使用して AWS Elemental MediaLive チャネルからコンテンツを受信する AWS Elemental MediaConnect ように を設定できます。これにより、MediaLive から MediaConnect へのライブビデオの安全で信頼性の高い転送を確立し、さらなる配信や処理を行うことができます。

このページでは、「SRT 発信者出力グループの作成」で説明されているように、MediaLive から SRT 出力を受信するように を設定する責任について説明します。 https://docs.aws.amazon.com/medialive/latest/ug/opg-srt-caller.html

計画

開始する前に、次の点を考慮してください。

- the section called “アップストリームシステムとの調整”
- the section called “Amazon VPC を使用して配信を計画する”

アップストリームシステムとの調整

ユーザーと MediaLive オペレーターは、以下の点に同意する必要があります。

- チャネル設定 - 使用する MediaLive チャネルのタイプを決定します。
  - MediaLive チャンネルが標準チャンネルの場合は、2 つのフローソースが必要です。
  - MediaLive チャンネルが単一パイプラインチャンネルの場合は、1 つのフローソースが必要です。
- レイテンシー - ストリームの適切なレイテンシーを決定します。
  - MediaLive 設定に近いレイテンシー値を選択することをお勧めします。
  - MediaLive のソースにストリーム ID を含める場合は、MediaLive オペレータにその ID を知らせます。
- 暗号化アルゴリズム - 適切なアルゴリズムを決定します。
  - 使用する暗号化アルゴリズムには、AES 128、AES 192、AES 256 のいずれかに同意する必要があります。
- 暗号化パスフレーズ - 使用するパスフレーズを決定します。
  - パスフレーズは 10～79 文字の Unicode 文字です。つまり、スペースを使用できます。

Amazon VPC を使用して配信を計画する

Secrets Manager に関する考慮事項

VPC で実行されている MediaLive チャネル出力に接続する場合、SRT 出力は常に暗号化され、AWS Secrets Manager 統合が必要であることに注意してください。その結果、MediaLive チャネル出力は、次の特性を持つサブネットになります。

- チャネル出力のサブネットには Secrets Manager エンドポイントが必要です。
- チャネル出力と Secrets Manager エンドポイントのサブネットは、同じセキュリティグループを使用する必要があります。

MediaLive に関する考慮事項

MediaLive からコンテンツを受信する場合、MediaLive チャネル出力と MediaConnect フローソースは、同じ VPC 内または異なる VPCs内に配置できます。通常、同じ VPC を共有しますが、別々の VPC セキュリティグループで異なるサブネットを使用します。次の点に注意してください:

- 両方のサービスが同じ にある場合 AWS アカウント、同じ Secrets Manager シークレットを使用できます。MediaLive と MediaConnect が異なる VPCs またはサブネットにあるだけで、シークレットを複製する必要はありません。
- サービスが異なる場合 AWS アカウント、各演算子は通常、それぞれの でシークレットを個別にセットアップします AWS アカウント。

タスク

MediaLive から SRT 出力を受け取るには、次のタスクを完了する必要があります。

- the section called “1. 暗号化用のシークレットをリクエストする”
- the section called “2. SRT リスナーを使用して MediaConnect フローを作成する”
- the section called “3. MediaLive ソース IP を使用して MediaConnect MediaConnect フローの許可リストを設定する IPs”
- the section called “4. フローとチャネルを開始する”

1. 暗号化用のシークレットをリクエストする

適切なアクセス許可を持つ組織内のユーザーは、合意済みの SRT 暗号化パスフレーズを Secrets Manager のシークレットに保存する必要があります。

シークレットをリクエストするには

1. 1 つまたは 2 つのシークレットが必要かどうかを判断します。
   - MediaConnect と MediaLive が同じ にある AWS アカウント場合: 両方のサービスが使用する共有シークレットは 1 つだけ必要です。
   - MediaConnect と MediaLive が異なる にある AWS アカウント場合: 通常、各オペレーターは共有シークレットを使用するのではなく AWS アカウント、それぞれの で同じシークレットを個別にセットアップします。
2. MediaLive オペレーターと調整し、シークレットの作成をリクエストするユーザーについて合意します。
3. シークレットの作成を担当している場合は、必要なシークレットごとに以下の手順に従ってください。
   - 他のタイプをシークレットタイプとして使用して、Secrets Manager でシークレットを作成するように AWS 管理者に依頼します。
   - 合意済みの SRT 暗号化パスフレーズを AWS 管理者に付与して、シークレットに保存します。
   - AWS 管理者に以下の情報を提供するよう依頼してください。
     - シークレットの名前
     - シークレットの ARN は次のようになります。
       `arn:aws:secretsmanager:region:123456789012:secret:Sample-abcdef`
4. 1 つの共有シークレットを使用している場合は、MediaConnect 演算子と MediaLive 演算子の両方がシークレットの詳細を受信していることを確認します。

2. SRT リスナーを使用して MediaConnect フローを作成する

MediaLive からコンテンツを受信するには、MediaConnect MediaConnect フローを設定する必要があります。その後、フローからインバウンド IP アドレスを取得し、MediaLive オペレータに渡すことができます。MediaLive オペレータは、チャネルの設定にこれを必要とします。

フローをセットアップしてインバウンド IP アドレスを検索するには

1. MediaConnect コンソールを開きます。
2. 以下の手順に従って、フローを作成するか、これらの特定の設定で既存のフローを編集します。
   - ソースタイプ: ネットワーク設定に基づいて標準ソースまたは VPC ソースを選択します。
   - プロトコル: SRT リスナーを選択します。
   - ソースの説明: わかりやすい名前を入力します。

     > **Tip**
     >
     > MediaLive が 2 つのソースを送信している場合は、このフィールドを使用して各ソースを区別します。例えば、**`source-pipeline-0`** と **`source-pipeline-1`** です。

   - (標準ソースのみ):
     - 許可リスト CIDR ブロック: 一時値 (など**`192.168.76.54/32`**) を入力します。これは、後で実際の MediaLive チャネル IP アドレスで更新します。
   - (VPC ソースのみ):
     - VPC インターフェイス名: VPC インターフェイスを指定します。
     - サブネット: MediaConnect で使用する VPC サブネットを選択します。
     - セキュリティグループ: MediaConnect で使用する VPC セキュリティグループを指定します。
   - ポート: 1 ~ 65535 のポート番号を入力します。
   - 最大レイテンシー: 合意された値を入力します。
   - 暗号化: 暗号化を有効にするを選択します。
   - ロール ARN: Secrets Manager へのアクセス許可を持つロールを指定します。
   - シークレット ARN: 前のタスク () のシークレットの ARN を入力しますthe section called “1. 暗号化用のシークレットをリクエストする”。
3. フローを設定したら、フローの詳細ページでソースタブを見つけます。
4. インバウンド IP アドレス値を書き留めます。例えば、`srt://203.0.113.22:5000`、`srt://203.0.113.88:5001` です。
5. この IP アドレスを MediaLive 演算子に渡します。MediaLive オペレータは、MediaConnect フローを指す SRT 発信者出力グループを持つチャネルを作成できるようになりました。

3. MediaLive ソース IP を使用して MediaConnect MediaConnect フローの許可リストを設定する IPs

MediaLive チャネルを作成したら、チャネルからのトラフィックを受け入れるように MediaConnect フローを設定する必要があります。

フローを設定するには

1. MediaLive オペレータに、チャネルからのソース IP アドレスを尋ねます。
   - 標準 MediaLive チャネルの場合: 両方のソース IP アドレスをリクエストします。
   - 単一パイプラインチャネルの場合: 単一のソース IP アドレスをリクエストします。
   - MediaLive Anywhere チャネルの場合: チャネルが実行されているネットワークにゲートウェイ IP アドレスをリクエストします。
2. IP アドレスがある場合 :
   - MediaConnect コンソールに移動し、フローを開きます。
   - Sources タブに移動し、SRT ソースを選択します。
   - [更新] を選択します。
   - 「許可リスト CIDR ブロック」に、ソース IP を CIDR ブロックとして入力します (例: **`203.0.113.1/32`**)。
   - [更新] を選択します。

> **Note**
>
> - ソースが 2 つある場合は、各 IP アドレスを正しいソースに適用します。
> - IP アドレスには、 **`pipeline 0`**および というラベルが付いている場合があります**`pipeline 1`**。
> - 前のタスク () の例に従った場合the section called “2. SRT リスナーを使用して MediaConnect フローを作成する”、 **`pipeline 0`**はソースの説明フィールドに があるフロー**`source-pipeline-0`**ソースに対応します。

4. フローとチャネルを開始する

フローとチャネルの両方を設定したら、MediaLive から MediaConnect へのコンテンツフローを開始できるようになりました。

フローとチャネルを開始するには

1. MediaConnect コンソールで、フローを開始します。
2. フローがアクティブになった後 (これには約 1 分かかります)、MediaLive オペレーターにチャネルを開始できることを伝えます。
3. 両方が実行されると、MediaLive チャネルは MediaConnect フローへのコンテンツの送信を開始します。

トラブルシューティング

このワークフローで問題が発生した場合は、このチェックリストを使用して一般的な問題を特定して解決します。

- 両方のサービスが同じ暗号化パスフレーズを使用していることを確認します。
- MediaConnect フローの許可リストに正しい MediaLive チャネル IP アドレスが含まれていることを確認します。
- 両方のサービスに、シークレットにアクセスするために必要なアクセス許可があることを確認します。
- MediaLive 送信先 URL で指定されたポートが MediaConnect フローのポートと一致することを確認します。
- VPC のセットアップでは、セキュリティグループが必要なトラフィックを許可していることを確認します。

AWS Elemental MediaConnect におけるプロトコル

AWS Elemental MediaConnect は、使用するフローのタイプに応じて、受信 (ソース) ライブ動画ストリームと送信 (出力) ライブ動画ストリームのさまざまなプロトコルをサポートします。

マックスされた圧縮コンテンツ (オーディオ、動画、補助データを組み合わせたもの) を 1 つのストリームに転送するトランスポートストリームフローでは、次のプロトコルを使用します。

- 信頼性の高いインターネットストリームトランスポート (RIST) (シンプルプロファイルのみ) は、長距離アプリケーションに適した、可用性が高く低レイテンシーのプロトコルです。MediaConnect は、RIST プロトコルを使用するソースまたは出力の暗号化をサポートしていません。
- リアルタイム転送プロトコル (RTP) は RTP-FEC よりも適用範囲が広く、使用する帯域幅も少なくて済みます。MediaConnect は、RTP プロトコルを使用するソースまたは出力の暗号化をサポートしていません。
- フォワードエラー訂正機能付きリアルタイム転送プロトコル (RTP-FEC) は適用範囲が広く、フォワードエラー訂正 (FEC) により破損やパケット損失を自己修復します。このプロトコルを使用すると、FEC を使用しない RTP よりも多くの帯域幅が必要になります。AWS Elemental MediaConnect は、RTP-FEC プロトコルを使用するソースまたは出力の暗号化をサポートしていません。
- セキュアリライアブルトランスポート (SRT) は、長距離アプリケーションに適した、可用性が高く低レイテンシーのプロトコルです。
  - SRT リスナーは SRT プロトコルをプルベースで実装したものです。SRT リスナーはソースまたは出力として使用できます。SRT リスナーは SRT 発信者と通信する必要があります。
  - SRT コーラーは SRT プロトコルのプッシュベースの実装です。SRT 発信者はソースまたは出力として使用できます。SRT 発信者は SRT リスナーと通信する必要があります。
- Zixi は可用性の高いプロトコルで、ほとんどのアプリケーション、特に長距離のユースケースに適しています。お使いのエンコーダーが Zixi に対応していない場合は、MediaConnect 専用に作成された Zixi フィーダー/レシーバーソフトウェアを使用できます。このソフトウェアには Zixi の Web サイトからアクセスできます。ダウンロードする前に、情報の入力を求められます。配信用に複数のフローを設定する場合は、フロー間でコンテンツを送信するプロトコルとして Zixi を使用することをおすすめします。MediaConnect は、次の 2 つの Zixi プロトコルオプションをサポートしています。
  - Zixi プル は Zixi プロトコルを使用して、ファイアウォールの内側にあるレシーバーまたは統合レシーバーデコーダー (IRD) にコンテンツを送信します。また、MediaConnect からレシーバー

にトラフィックをルーティングするためにネットワークアドレス変換 (NAT) が必要な場合にもこのオプションを使用できます。

- Zixi プッシュ は Zixi プロトコルを使用して、公開アドレス可能な静的 IP アドレスを持つレシーバーにコンテンツを送信します。このオプションは、レシーバーがファイアウォールや NAT ベースのルーターの背後にいない場合に使用します。
- Zixi プッシュ for AWS Elemental Link は、Zixi プッシュプロトコルを使用して AWS Elemental Link UHD デバイスを MediaConnect フローに接続します。

- Fujitsu-QoS は、低レイテンシー、高スループットの富士通独自のプロトコルで、富士通デバイスからMediaConnect へ、および MediaConnect から富士通デバイスへの転送を可能にします。富士通プロトコルを使用する場合、MediaConnect はソースフェイルオーバーをサポートしません。

JPEG XS を使用して軽く圧縮された高品質のコンテンツを転送する CDI フローでは、次のプロトコルを使用します。

- AWS Cloud Digital Interface (AWS CDI) は、高い信頼性と最低 8 ミリ秒のネットワークレイテンシーで、AWS高品質の非圧縮動画をクラウド内で転送できるようにするテクノロジーです。
- ST 2110 JPEG XS は、最小限の圧縮でストリームで使用できる低レイテンシーのプロトコルです。

ソースと出力のプロトコルサポート

次の表は、ソース、出力、またはその両方に使用できるプロトコルをまとめたものです。

トランスポートストリームプロトコル

プロトコル	これをソースとして使用できますか?	これを出力として使用できますか?
RIST	はい	はい
RTP	はい	はい
RTP-FEC	はい	はい
SRT リスナー	はい	はい
SRT コーラー	はい	はい

プロトコル	これをソースとして使用できますか?	これを出力として使用できますか?
Zixi プル	いいえ	はい
Zixi プッシュ	はい	はい
Fujitsu-QoS	はい	はい

CDI プロトコル

プロトコル	これをソースとして使用できますか?	これを出力として使用できますか?
CDI	はい	はい
ST 2110 JPEG XS	はい	はい

CDI プロトコルのカラーサポート

MediaConnect CDI フローは、プロトコルごとにカラースペース、ビット深度、クロマサンプリングの複数の構成をサポートします。次の表では、各 CDI プロトコルでサポートされる構成について説明しています。

> **Note**
>
> MediaConnect は現在 CDI 入力の RGB カラースペースをサポートしていません。MediaConnect から MediaConnect に CDI フローを出力する場合は、必ず YCbCr カラースペースを使用してください。

CDI カラーサポート

プロトコル	サポートされるカラー設定
CDI	• YCbCr 10 ビット 4:2:2 • RGB 10 ビット 4:4:4

プロトコル	サポートされるカラー設定
	• RGB 12 ビット 4:4:4
ST 2110 JPEG XS	• YCbCr 10 ビット 4:2:2 • RGB 10 ビット 4:4:4 • RGB 12 ビット 4:4:4

のセキュリティ AWS Elemental MediaConnect

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、 AWS とお客様の間の責任共有です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – クラウドで AWS AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。「AWS 」 コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。「 AWS Elemental MediaConnect」 に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の 「AWS 」 のサービス」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Elemental MediaConnect。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成する AWS Elemental MediaConnect ように を設定する方法を示します。また、 AWS Elemental MediaConnect リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- AWS Elemental MediaConnect でのデータの保護
- AWS Elemental MediaConnect でのアイデンティティ管理とアクセス管理
- ログ記録とモニタリング
- のコンプライアンス検証 AWS Elemental MediaConnect
- の耐障害性 AWS Elemental MediaConnect
- のインフラストラクチャセキュリティ AWS Elemental MediaConnect

AWS Elemental MediaConnect でのデータの保護

が提供するツールを使用してデータを保護できます AWS。AWS Elemental MediaConnect は、受信動画 (ソース) を復号化し、送信動画 (出力と使用権限) を暗号化できます。

転送中のコンテンツを暗号化するには、次の 3 つのオプションがあります。

- スタティックキー暗号化: このオプションを使用して、ソース、出力、使用権限を暗号化できます。暗号化キーを に保存し AWS Secrets Manager、Secrets Manager から暗号化キーを取得するアクセス許可を MediaConnect に付与します。

  利点: アカウントの暗号化キーの保存を完全に制御できます。キーは に保存され AWS Secrets Manager、いつでもアクセスできます。

  問題点: すべての関係者 (ソース、フロー、出力、使用権限の所有者) が暗号化キーが必要です。使用権限を使用してコンテンツを共有する場合、作成者とサブスクライバーの両方が暗号化キーを AWS Secrets Managerに保存する必要があります。暗号化キーが変更された場合は、すべての関係者に新しいキーを通知する必要があります。
- セキュアパッケージャーエンコーダーキー交換 (SPEKE): このオプションを使用して、使用権限を介して送信されるコンテンツを暗号化できます。暗号化キーを管理および提供する条件付きアクセス (CA) プラットフォームキープロバイダーと提携します。次に、CA プラットフォームキープロバイダーと AWS アカウント間のプロキシとして機能するアクセス許可を Amazon API Gateway に付与します。

  利点: コンテンツ作成者は、暗号化キーへのアクセスを完全に制御できます。コンテンツ作成者は、暗号化キーを管理する CA プラットフォームキープロバイダと提携しますが、キー自体を扱うことはなく、他の当事者と共有することもありません。キープロバイダーの機能によっては、このオプションにより暗号化キーに時間制限を割り当てたり、キーを完全に取り消したりすることができます。サブスクライバーは暗号化を設定する必要はありません。この情報は使用権限を通じて自動的に提供されます。

  問題点:サードパーティ (キープロバイダー) と協力する必要があります。
- セキュアリライアブルトランスポート (SRT) パスワード暗号化: SRT プロトコルを使用する場合、このオプションを使用してソースと出力を暗号化できます。SRT プロトコルは、長距離アプリケーションに適した、可用性が高く低レイテンシーのプロトコルです。暗号化パスワードを AWS Secrets Managerに保存し、Secrets Manager から暗号化パスワードを取得する権限を MediaConnect に付与します。

利点: 暗号化と復号化に 128/256 ビット AES を使用します。SRT プロトコルは、エラー訂正を使用してパケットロスを最小限に抑えます。暗号化パスワードの保存に関し、完全に制御できます。パスワードは に保存され AWS Secrets Manager、いつでもアクセスできます。

問題点: SRT プロトコルでのみ使用可能です。SRT プロトコルを使用する場合、MediaConnect はソースフェイルオーバーをサポートしません。

> **Note**
>
> 暗号化は、使用権限、Zixi または SRT プロトコルを使用するソース、および Zixi または SRT プロトコルを使用する出力でのみサポートされます。

トピック

AWS Elemental MediaConnect での静的キーの暗号化

静的キー暗号化を使用してソース、出力、およびエンタイトルメントを保護することができます。暗号化キーを に保存し AWS Secrets Manager、Secrets Manager から暗号化キーを取得するアクセス許可を MediaConnect に付与します。

トピック

スタティックキー暗号化のキー管理

AWS Elemental MediaConnect では、スタティックキー暗号化を使用して、ソース、出力、および使用権限のコンテンツを保護できます。この方法を使用するには、暗号化キーをシークレットとして に保存し AWS Secrets Manager、シークレットへのアクセス許可を AWS Elemental

MediaConnect に付与します。Secrets Manager は暗号化キーを安全に保ち、 AWS Identity and Access Management (IAM) ポリシーで指定したエンティティのみがアクセスできるようにします。

スタティックキー暗号化では、すべての参加者 (ソース、フロー、出力や使用権限の所有者) が暗号化キーを必要とします。エンタイトルメントを使用してコンテンツを共有する場合、両方の AWS アカウント所有者が暗号化キーを保存する必要があります AWS Secrets Manager。

詳細については、「スタティックキー暗号化の設定」を参照してください。

AWS Elemental MediaConnect を使用したスタティックキー暗号化のセットアップ

暗号化されたソース、またはスタティックキー暗号化を使用する出力または使用権限を含むフローを作成する前に、次の手順を実行する必要があります。

ステップ 1 — 暗号化キーをシークレットとして AWS Secrets Managerに保存します。

ステップ 2 — AWS Elemental MediaConnect が AWS Secrets Managerに保存されたシークレットを読み取ることを許可する IAM ポリシーを作成します。

ステップ 3 — IAM ロールを作成し、ステップ 2 で作成したポリシーをアタッチします。次に、AWS Elemental MediaConnect を信頼できるエンティティとして設定します。このエンティティは、このロールを引き受け、アカウントに代わってリクエストを行うことが許可されます。

> **Note**
>
> MediaConnect は、使用権限に対して、また Zixi および SRT プロトコルを使用するソースと出力に対しての暗号化のみをサポートします。Secrets Manager に保存されている Zixi プロトコルのキーは、16 進形式の静的キーです。SRT はパスキーを使用して暗号化します。

ステップ 1: 暗号化キーを に保存する AWS Secrets Manager

静的キー暗号化を使用して AWS Elemental MediaConnect コンテンツを暗号化するには、 AWS Secrets Manager を使用して暗号化キーを保存するシークレットを作成する必要があります。シークレットと、同じ AWS アカウントのシークレットを使用するリソース (ソース、出力、または使用権限) を作成する必要があります。シークレットはアカウント間で共有できません。

> **Note**
>
> 2 つのフローを使用して 1 つの AWS リージョンから別のリージョンにビデオを配信する場合は、2 つのシークレット (各リージョンに 1 つのシークレット) を作成する必要があります。

Secrets Manager に暗号化キーを保存するには

1. ソースを管理するエンティティから暗号化キーを取得します。
2. https://console.aws.amazon.com/secretsmanager/ で AWS Secrets Manager コンソールにサインインします。
3. [Store a new secret] (新しいシークレットの保存) ページの [Select secret type] (シークレットタイプの選択) で、[Other type of secrets] (他の種類のシークレット) を選択します。
4. キー/値のペア では、プレーンテキスト を選択します。
5. ボックス内のテキストをすべて消去し、暗号化キーの値のみに置き換えます。16 進キーの場合は、キーの長さをチェックして、暗号化タイプに指定された長さと一致することを確認してください。例えば、AES-256 暗号化キーは 64 桁である必要があります。これは、各桁のサイズが 4 ビットであるためです。
6. [Select the encryption key] (暗号化キーの選択) は、デフォルト設定の [DefaultEncryptionKey] のままにします。
7. [次へ] を選択します。
8. [シークレット名] には、後で識別しやすいシークレットの名前を指定します。例えば、**`2018-12-01_baseball-game-source`**。
9. [次へ] を選択します。
10. [Configure automatic rotation] (自動ローテーションの設定) セクションで、[Disable automatic rotation] (自動ローテーションを有効化する) を選択します。
11. [Next] (次へ) を選択してから、[Store] (保存) を選択します。

    新しいシークレットの詳細ページが表示され、シークレット ARN などの情報が表示されます。
12. Secrets Manager のシークレット ARN を書き留めます。この情報は、次の手順で必要になります。

ステップ 2: AWS Elemental MediaConnect にシークレットへのアクセスを許可する IAM ポリシーを作成する

ステップ 1 では、シークレットを作成して AWS Secrets Managerに保存しました。このステップでは、保存したシークレットを読み取ることをAWS Elemental MediaConnect に許可する IAM ポリシーを作成します。

MediaConnect にシークレットへのアクセスを許可する IAM ポリシーを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインから、[Policies] (ポリシー) を選択します。
3. ポリシーの作成 を選択し、JSON タブを選択します。
4. 以下のフォーマットを使用するポリシーを入力します。

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-west-2:111122223333:secret:aes256-7g8H9i"
      ]
    }
  ]
}
```

   Resource セクションでは、各行は作成した異なるシークレットの ARN を表しています。その他の例については、「Secrets Manager で MediaConnect 暗号化キーにアクセスするためのポリシー例」を参照してください。

5. [ポリシーの確認] を選択します。

6. 名前 にポリシーの名前を入力します (例: **SecretsManagerForMediaConnect**)。
7. [Create policy] (ポリシーの作成) を選択します。

ステップ 3: 信頼できる関係を持つ IAM ロールを作成する

ステップ 2 では、 AWS Secrets Managerに保存したシークレットへの読み取りアクセスを許可する IAM ポリシーを作成しました。この手順では、IAM ロールを作成し、このポリシーをロールに割り当てます。次いで、AWS Elemental MediaConnect を、ロールを引き受け可能な信頼できるエンティティとして定義します。これにより、MediaConnect はシークレットへの読み取りアクセス権を持つことができます。

信頼関係のあるロールを作成するには

1. IAM コンソールのナビゲーションペインで [ロール] を選択します。
2. [Role] (ロール) ページで、[Create role] (ロールの作成) を選択します。
3. [ロールを作成] ページの 信頼されたエンティティのタイプを選択 セクションで、[AWS サービス] (デフォルト)を選択します 。
4. [Choose the service that will use this role] (このロールを使用するサービスを選択) で、[EC2] を選択します。

   EC2 を選択する理由は、現在、AWS Elemental MediaConnect はリストに含まれていないためです。EC2 を選択すると、ロールを作成できます。後の手順で、このロールを変更し、EC2 を MediaConnect に置き換えます。
5. [Next: Permissions] (次のステップ: 許可) を選択します。
6. [許可ポリシーをアタッチ] には、ステップ 2 で作成したポリシーの名前 (**SecretsManagerForMediaConnect** など) を入力してください。
7. SecretsManagerReadWrite の場合は、チェックボックスをオンにして、次へ: レビュー を選択します。
8. [Role name] (ロール名) に名前を入力します。`MediaConnectAccessRole` は留保されているため、この名前は使用しないことを強くお勧めします。代わりに、`MediaConnect` を含み、このロールの目的を説明する名前を使用します (例: **MediaConnect-ASM**)。
9. ロールの説明 では、デフォルトのテキストをこのロールの目的を覚えるのに役立つ説明に置き換えます。例: **Allows MediaConnect to view secrets stored in AWS Secrets Manager.**
10. [ロールの作成] を選択してください。

11. ページの上部に表示される確認メッセージで、作成したロール名を選択します。
12. [信頼関係] を選択し、[信頼ポリシーの編集] を選択してください。
13. [信頼ポリシーの編集] ウィンドウで、JSON を次のように変更します。

    - [サービス] で、`ec2.amazonaws.com` を `mediaconnect.amazonaws.com` に変更します。
    - セキュリティを強化するには、信頼ポリシーに特定の条件を定義します。これにより、MediaConnect はアカウント内のリソースのみを使用するように制限されます。これを行うには、[アカウント ID]、[フロー ARN]、またはその両方などのグローバル条件を使用します。以下の信頼ポリシーの例を参照してください。グローバル条件によるセキュリティ上の利点の詳細については、「サービス間での混乱した代理問題の防止」を参照してください。

      > **Note**
      >
      > 次の例では、[アカウント ID] と [フロー ARN] 条件の両方を使用しています。両方の条件を使用しないと、ポリシーの見え方が変わります。フローの完全な ARN が不明な場合や、複数のフローを指定する場合には、グローバルコンテキスト条件キー `aws:SourceArn` で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば、`arn:aws:mediaconnect:*:111122223333:*`。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "mediaconnect.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:mediaconnect:us-
west-2:111122223333:flow:*:flow-name"
                }
```

```
            }
        }
    ]
}
```

14. [Update Trust Policy] (信頼ポリシーの更新) を選択します。
15. [Summary] (概要) ページで、[Role ARN] (ロール ARN) の値をメモします。以下のような形式です：`arn:aws:iam::111122223333:role/MediaConnectASM`

AWS Elemental MediaConnect での SPEKE の暗号化

Secure Packager and Encoder Key Exchange (SPEKE) を AWS Elemental MediaConnect で使用することで、使用権限 を暗号化できます。これにより、コンテンツの作成者は、このコンテンツに対するアクセス権限を完全に制御できます。この使用法は、「SPEKE ドキュメント」に記載されている SPEKE クラウドベースのアーキテクチャをカスタマイズしたものです。

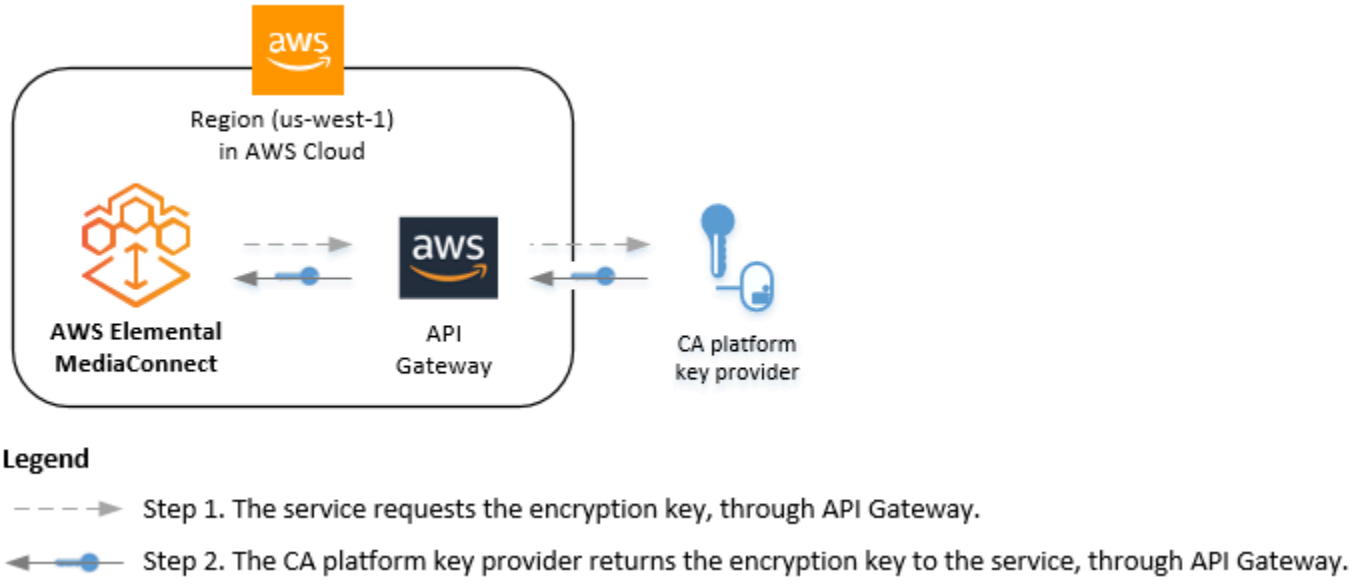
トピック

- SPEKE のキー管理
- AWS Elemental MediaConnect を使用した SPEKE 暗号化の設定

SPEKE のキー管理

SPEKE を実装すると、条件付きアクセス (CA) システムが AWS Elemental MediaConnect にキーを提供し、コンテンツの暗号化と復号化を行います。API ゲートウェイは、サービスと CA プラットフォームキープロバイダ間の通信のプロキシとして機能します。各 AWS Elemental MediaConnect フローは、API Gateway プロキシと同じ AWS リージョンに存在する必要があります。

次の図は、AWS Elemental MediaConnect が SPEKE を使用して暗号化キーまたは復号キーを取得する方法を示しています。発信者のフローでは、サービスは暗号化キーを取得し、それを使用してコンテンツを暗号化してから、使用権限を通じて送信します。サブスクライバーのフローでは、サービスは使用権限からコンテンツを受信したときに復号化キーを取得します。



以下に主なサービスとコンポーネントを示します。

- AWS Elemental MediaConnect — フローの暗号化設定を提供および制御します。AWS Elemental MediaConnect は、Amazon API Gateway を通じて CA プラットフォームキープロバイダーから暗号化キーを取得します。AWS Elemental MediaConnect は、暗号化キーを使用してコンテンツを暗号化するか (発信者のフローの場合)、コンテンツを復号化します (サブスクライバーのフローの場合)。
- API Gateway – エンクリプタとキープロバイダーの間でお客様に信頼されるロールとプロキシ通信を管理します。API ゲートウェイではロギング機能が利用でき、お客様はエンクリプタおよび CA プラットフォームとの関係を管理できます。API Gateway は、エンクリプタと同じ AWS リージョンに存在する必要があります。
- CA プラットフォームキープロバイダー — SPEKE 準拠 API を通じて AWS Elemental MediaConnect に暗号化キーと復号キーを提供します。

詳細については、「SPEKE 暗号化の設定」を参照してください。

AWS Elemental MediaConnect を使用した SPEKE 暗号化の設定

SPEKE 暗号化を使用する使用権限を付与する前に、次のステップを実行する必要があります。

ステップ 1. — 暗号化キーを管理する条件付きアクセス (CA) プラットフォームキープロバイダーに依頼します。このプロセスでは、Amazon API Gateway で API を作成します。この API は、AWS Elemental MediaConnect に代わってリクエストをキープロバイダーに送信します。

ステップ 2 — ステップ 1 で作成した API がキープロバイダーにリクエストを行うためのプロキシとして機能することを許可する IAM ポリシーを作成します。

ステップ 3. — IAM ロールを作成し、ステップ 2 で作成したポリシーをアタッチします。次に、AWS Elemental MediaConnect を、このロールを引き受け、ユーザーに代わって API Gateway エンドポイントにアクセスすることが許可される、信頼できるエンティティとして設定します。

ステップ 1: CA プロバイダーとのオンボーディング

AWS Elemental MediaConnect で SPEKE を使用するには、CA プラットフォームキープロバイダーが必要です。以下の AWS パートナーは、SPEKE の MediaConnect カスタマイズのための条件付きアクセス (CA) ソリューションを提供します。

- Verimatrix

コンテンツ作成者の場合は、CA プラットフォームのキープロバイダーに連絡して、オンボーディングプロセスの支援を受けてください。CA プラットフォームキープロバイダの助けを借りて、誰がどのコンテンツにアクセスできるかを管理できます。

オンボーディングプロセス中は、以下の点に注意してください。

- **POST** メソッドリクエストの ARN — API ゲートウェイで作成したリクエストに AWS が割り当てる Amazon リソースネーム (ARN)。
- 定数初期化ベクトル (オプション) — コンテンツを暗号化するためのキーで使用する、32 文字の文字列により表示される 128 ビット (16 バイト) の 16 進値。
- デバイス ID — キープロバイダーで設定する各デバイスの固有識別子。各デバイスはコンテンツの異なる受信者を表します。
- リソース ID — キープロバイダーとともに構成するコンテンツごとに作成する一意の識別子。
- URL — Amazon API Gateway で作成した API に AWS により割り当てられた URL。

これらの値は、後で MediaConnect で 使用権限 を設定するときに必要になります。

ステップ 2: API ゲートウェイをプロキシとして動作させる IAM ポリシーを作成する

ステップ 1 では、暗号化キーを管理する CA プラットフォームキープロバイダーと協力しました。このステップでは、API ゲートウェイがユーザーに代わってリクエストを行うことを許可する IAM ポリシーを作成します。API ゲートウェイは、アカウントとキープロバイダ間の通信のプロキシとして機能します。

API ゲートウェイプロキシの IAM ポリシーを作成するには

1. IAM コンソールのナビゲーションペインから、[Policies] (ポリシー) を選択します。
2. ポリシーの作成 を選択し、JSON タブを選択します。
3. 以下のフォーマットを使用するポリシーを入力します。

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "execute-api:Invoke"
      ],
      "Resource": [
        "arn:aws:execute-api:us-west-2:111122223333:1abcdefghi/*/POST/*"
      ]
    }
  ]
}
```

   `Resource` セクションで、サンプルの Amazon リソースネーム (ARN) を、CA プラットフォームキープロバイダーを使用して API ゲートウェイ `POST` で作成したメソッドリクエストの ARN に置き換えます。

4. [Review policy] (ポリシーの確認) を選択します。
5. [Name] (名前) に **`APIGateway-Proxy-Access`** と入力します。
6. [ポリシーの作成] を選択します。

ステップ 3: 信頼できる関係を持つ IAM ロールを作成する

ステップ 2 では、API ゲートウェイがプロキシとして機能し、ユーザーに代わってリクエストを行うことを許可する APIGateway プロキシアクセス ポリシーを作成しました。このステップでは、IAM ロールを作成し、以下のアクセス許可をアタッチします。

- APIGateway プロキシアクセス ポリシーにより、Amazon API Gateway がユーザーに代わってプロキシとして機能し、アカウントと CA プラットフォームキープロバイダとの間でリクエストを行うことができます。これは ステップ 1 で作成したポリシーです。
- 信頼関係 ポリシーにより、AWS Elemental MediaConnect がユーザーに代わってロールを引き受けることができます。このポリシーは次の手順の一部として作成します。

信頼できる関係を持つ IAM ロールを作成するには

1. IAM コンソールのナビゲーションペインで [ロール] を選択します。
2. [Role] (ロール) ページで、[Create role] (ロールの作成) を選択します。
3. [ロールを作成] ページの 信頼されたエンティティのタイプを選択 セクションで、[AWS サービス] (デフォルト)を選択します 。
4. [Choose the service that will use this role] (このロールを使用するサービスを選択) で、[EC2] を選択します。

   EC2 を選択する理由は、現在、AWS Elemental MediaConnect はリストに含まれていないためです。EC2 を選択すると、ロールを作成できます。後の手順で、このロールを変更し、EC2 を MediaConnect に置き換えます。
5. [Next: Permissions] (次のステップ: 許可) を選択します。
6. フィルターポリシー で、顧客が管理するポリシー を選択します。
7. APIGateway プロキシアクセス の横にあるチェックボックスを選択し、次へ: タグ を選択します。
8. タグ値 (オプション) を入力し、次へ: レビューを選択します。
9. ロール名 に、**SpekeAccess** など、名前を入力します。
10. ロールの説明 では、デフォルトのテキストをこのロールの目的を覚えるのに役立つ説明に置き換えます。例: **Allows AWS Elemental MediaConnect to talk to API Gateway on my behalf.**
11. [ロールの作成] を選択してください。
12. ページの上部に表示される確認メッセージで、作成したロール名を選択します。
13. 信頼関係 を選択し、信頼関係の編集 を選択します。
14. ポリシードキュメント では、ポリシーを次のように変更します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "mediaconnect.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

15. [Update Trust Policy] (信頼ポリシーの更新) を選択します。
16. [Summary] (概要) ページで、[Role ARN] (ロール ARN) の値をメモします。以下のような形式です：`arn:aws:iam::111122223333:role/SpekeAccess`

AWS Elemental MediaConnect の SRT パスワード暗号化

SRT プロトコルを使用する場合、Secure Reliable Transport (SRT) パスワード暗号化オプションを使用してソースと出力を暗号化できます。SRT プロトコルは可用性が高く低レイテンシーのプロトコルで、長距離アプリケーションに適しています。暗号化パスワードを に保存し AWS Secrets Manager、Secrets Manager から暗号化パスワードを取得するアクセス許可を MediaConnect に付与します。

トピック

- SRT パスワード暗号化のパスワード管理
- AWS Elemental MediaConnect を使用した SRT パスワード暗号化の設定

SRT パスワード暗号化のパスワード管理

AWS Elemental MediaConnect では、SRT パスワード暗号化を使用してソースと出力のコンテンツを保護できます。この方法を使用するには、SRT パスワードをシークレットとして に保存し AWS Secrets Manager、シークレットへのアクセス許可を AWS Elemental MediaConnect に付与しま

す。Secrets Manager はパスワードを安全に保ち、 AWS Identity and Access Management (IAM) ポリシーで指定したエンティティのみがアクセスできるようにします。

SRT パスワード暗号化では、すべての参加者 (ソース、フロー、および出力の所有者) に SRT パスワードが必要です。

詳細については、「SRT パスワード暗号化の設定」を参照してください。

AWS Elemental MediaConnect を使用した SRT パスワード暗号化の設定

暗号化されたソースや SRT パスワード暗号化を使用する出力を含むフローを作成する前に、次の手順を実行する必要があります。

ステップ 1 – SRT パスワードをシークレットとして保存します AWS Secrets Manager。

ステップ 2 — AWS Elemental MediaConnect が AWS Secrets Managerに保存されたシークレットを読み取ることを許可する IAM ポリシーを作成します。

ステップ 3 — IAM ロールを作成し、ステップ 2 で作成したポリシーをアタッチします。次に、AWS Elemental MediaConnect を信頼できるエンティティとして設定します。このエンティティは、このロールを引き受け、アカウントに代わってリクエストを行うことが許可されます。

ステップ 1: 暗号化パスワードを に保存する AWS Secrets Manager

SRT パスワード暗号化を使用して AWS Elemental MediaConnect コンテンツを暗号化するには、AWS Secrets Manager を使用してパスワードを保存するシークレットを作成する必要があります。シークレットと、同じ AWS アカウントのシークレットを使用するリソース (ソースまたは出力) を作成する必要があります。シークレットはアカウント間で共有できません。

> **Note**
>
> 2 つのフローを使用して 1 つの AWS リージョンから別のリージョンにビデオを配信する場合は、2 つのシークレット (各リージョンに 1 つのシークレット) を作成する必要があります。

出力を暗号化するために新しい SRT パスワードを作成する場合は、以下のパスワードポリシーをお勧めします。

- パスワードの文字数制限: 10 ~ 80 文字

- 大文字、小文字、数字、**! @ # $ % ^ & * ( ) _ + - = [ ] { } | '** 記号のうち、最低 3 つの文字タイプの組み合わせ
- AWS アカウント名または E メールアドレスと同じにしない

Secrets Manager にパスワードを保存するには

1. https://console.aws.amazon.com/secretsmanager/ で AWS Secrets Manager コンソールにサインインします。
2. [Store a new secret] (新しいシークレットの保存) ページの [Select secret type] (シークレットタイプの選択) で、[Other type of secrets] (他の種類のシークレット) を選択します。
3. キー/値のペア では、プレーンテキスト を選択します。
4. ボックス内のテキストをすべて消去し、SRT パスワードの 値 のみに置き換えます。
5. 暗号化 キーについては、デフォルトの設定を aws/secretsmanager のままにしてください。
6. [次へ] を選択します。
7. [シークレット名] には、後で識別しやすいシークレットの名前を指定します。例えば、**2018-12-01_baseball-game-source**。
8. [次へ] を選択します。
9. 自動ローテーションの設定 セクションでは、自動ローテーション を解除します。
10. [Next] (次へ) を選択してから、[Store] (保存) を選択します。次の画面で、作成したシークレットの名前を選択します。

    新しいシークレットの詳細ページが表示され、シークレット ARN などの情報が表示されます。
11. Secrets Manager のシークレット ARN を書き留めます。この情報は、次の手順で必要になります。

ステップ 2: AWS Elemental MediaConnect にシークレットへのアクセスを許可する IAM ポリシーを作成する

ステップ 1 では、シークレットを作成して AWS Secrets Managerに保存しました。このステップでは、保存したシークレットを読み取ることをAWS Elemental MediaConnect に許可する IAM ポリシーを作成します。

MediaConnect にシークレットへのアクセスを許可する IAM ポリシーを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

2. IAM コンソールのナビゲーションペインから、[Policies] (ポリシー) を選択します。
3. ポリシーの作成 を選択し、JSON タブを選択します。
4. 以下のフォーマットを使用するポリシーを入力します。

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-west-2:111122223333:secret:aes256-7g8H9i"
      ]
    }
  ]
}
```

   Resource セクションでは、各行は作成した異なるシークレットの ARN を表しています。前の手順のシークレット ARN を入力します。[Next: Tags (次へ: タグ)] を選択します。
5. [次へ: レビュー] を選択します。
6. 名前 にポリシーの名前を入力します (例: **SecretsManagerForMediaConnect**)。
7. [Create policy] (ポリシーの作成) を選択します。

ステップ 3: 信頼できる関係を持つ IAM ロールを作成する

ステップ 2 では、 AWS Secrets Managerに保存したシークレットへの読み取りアクセスを許可する IAM ポリシーを作成しました。この手順では、IAM ロールを作成し、このポリシーをロールに割り当てます。次いで、AWS Elemental MediaConnect を、ロールを引き受け可能な信頼できるエンティティとして定義します。これにより、MediaConnect はシークレットへの読み取りアクセス権を持つことができます。

信頼関係のあるロールを作成するには

1. IAM コンソールのナビゲーションペインで [ロール] を選択します。
2. [Role] (ロール) ページで、[Create role] (ロールの作成) を選択します。
3. [ロールを作成] ページの 信頼されたエンティティのタイプを選択 セクションで、[AWS サービス] (デフォルト)を選択します 。
4. [Choose the service that will use this role] (このロールを使用するサービスを選択) で、[EC2] を選択します。

   EC2 を選択する理由は、現在、AWS Elemental MediaConnect はリストに含まれていないためです。EC2 を選択すると、ロールを作成できます。後の手順で、このロールを変更し、EC2 を MediaConnect に置き換えます。
5. [Next: Permissions] (次のステップ: 許可) を選択します。
6. [許可ポリシーをアタッチ] には、ステップ 2 で作成したポリシーの名前 (**`SecretsManagerForMediaConnect`** など) を入力してください。
7. SecretsManagerForMediaConnect の場合は、チェックボックスを選択して 次へ を選択します。
8. [Role name] (ロール名) に名前を入力します。`MediaConnectAccessRole` は留保されているため、この名前は使用しないことを強くお勧めします。代わりに、`MediaConnect` を含み、このロールの目的を説明する名前を使用します (例: **`MediaConnect-ASM`**)。
9. ロールの説明 では、デフォルトのテキストをこのロールの目的を覚えるのに役立つ説明に置き換えます。例: **`Allows MediaConnect to view secrets stored in AWS Secrets Manager.`**
10. [ロールの作成] を選択してください。
11. ページの上部に表示される確認メッセージで、作成したロール名を選択します。
12. [信頼関係] を選択し、[信頼ポリシーの編集] を選択してください。
13. 信頼ポリシーの編集 では、`ec2.amazonaws.com` を `mediaconnect.amazonaws.com` に変更します。

    ポリシードキュメントは次のようになります。

    JSON

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "mediaconnect.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

14. [ポリシーの更新] を選択してください。
15. [Summary] (概要) ページで、[Role ARN] (ロール ARN) の値をメモします。以下のような形式です：`arn:aws:iam::111122223333:role/MediaConnectASM`

ネットワーク間のトラフィックのプライバシー

Amazon VPC と企業ネットワーク間のプライベート接続を設定するには、インターネット経由の IPsec VPN 接続または Direct Connect 接続を使用したプライベート物理接続のいずれかを設定できます。 Direct Connect を使用すると、オンプレミスネットワークから Amazon VPC に直接プライベート仮想インターフェイスを確立し、ネットワークと VPC 間にプライベートで高帯域幅のネットワーク接続を提供できます。複数の仮想インターフェイスを使用するため、ネットワーク分離が維持しながら、複数の VPC へのプライベート接続を確立できます。詳細については、「AWS Site-to-Site VPN とは」および「What is Direct Connect?」を参照してください。

MediaConnect と企業ネットワーク間のトラフィックを 仮想プライベートクラウド (VPC) 経由で直接ルーティングするには

1. Amazon VPC と企業ネットワークの間にプライベート接続を設定します。インターネット経由の IPsec VPN 接続か、接続を使用したプライベート物理 Direct Connect 接続のいずれかを選択できます。
2. VPC ソースを使用するフローを作成します。このプロセスでは、VPC インターフェイスをフローに追加してVPC とフロー間の初期接続を確立します。また、同じ VPC インターフェイスを新しいフローのソースとして指定します。

> **Note**
>
> フローがすでに存在する場合は、フローを更新して VPC インターフェイスを追加し、その VPC インターフェイスを使用する別のソースを追加できます。

AWS Elemental MediaConnect でのアイデンティティ管理とアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、認証を受ける(サインインする) ことができ、MediaPackage リソースの使用が承認(アクセス許可を付与) されるユーザーをコントロールします。IAM は、追加料金なしで使用できる AWS のサービス です。

対象者

AWS Identity and Access Management (IAM) の使用方法は、MediaConnect で行う作業によって異なります。

サービスユーザー: MediaConnect サービスを使用してジョブを実行するユーザーには、管理者が必要なアクセス許可と認証情報を提供します。作業を実行するために、さらに多くの MediaConnect の機能を使用する場合には、追加の許可が必要になることがあります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。MediaConnect の機能にアクセスできない場合は、「Elemental MediaConnect AWS のアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者: 企業内で MediaConnect リソースの管理を担当している方には、通常、MediaConnect への完全なアクセス権限が付与されます。どの従業員が MediaConnect のどの機能やリソースにアクセスできるかを決定するのは、管理担当者の役割です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。企業が MediaConnect で IAM を利用する方法については、「Elemental MediaConnect AWS と IAM の連携方法」を参照してください。

IAM 管理者: IAM 管理者の場合は、MediaConnect へのアクセスを管理するポリシーの作成方法について、詳細に把握しておきます。IAM で使用できる MediaConnect のID ベースのポリシーの例を確認するには、「AWS Elemental MediaConnect アイデンティティベースのポリシーの例」を参照してください。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けることによって、認証 (にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM アイデンティティセンター （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーション ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 AWS マネジメントコンソール または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストを暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用する AWS ことをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内の ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS マネジメントコンソール、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity

Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM アイデンティティセンター User Guide」の「Permission sets」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS マネジメントコンソール、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

その他のポリシータイプ

AWS は、一般的でない追加のポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の をグループ化して一元管理するためのサービス AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

詳細はこちら

MediaConnect 用 Identity and Access Management の詳細については、以下のページに進んでください。

- MediaConnect と IAM の連携方法
- アイデンティティベースのポリシーの例
- リソースベースのポリシーの例
- のシークレットのポリシー例 AWS Secrets Manager
- トラブルシューティング

Elemental MediaConnect AWS と IAM の連携方法

MediaConnect へのアクセスを管理するために IAM を使用する前に、MediaConnect でどの IAM 機能が使用できるかを理解しておく必要があります。MediaConnect およびその他の AWS のサービスが IAM と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

トピック

- MediaConnect での ID ベースのポリシー
- MediaConnect リソースベースのポリシー
- MediaConnect タグに基づく認可

- MediaConnect IAM ロール

MediaConnect での ID ベースのポリシー

IAM アイデンティティベースのポリシーでは許可または拒否するアクションとリソース、またアクションを許可または拒否する条件を指定できます。MediaConnect は、特定のアクション、リソース、および条件キーをサポートしています。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクション

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

MediaConnect のポリシーアクションでは、アクションの前にプレフィックス `mediaconnect:` が使用されます。例えば、MediaConnect `ListEntitlements` API オペレーションを使用して使用権限のリストを表示する許可を付与するには、そのポリシーに `mediaconnect:ListEntitlements` アクションを含めます。ポリシーステートメントには`Action` または `NotAction` 要素を含める必要があります。MediaConnect は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一のステートメントに複数のアクションを指定するには次のようにコンマで区切ります。

```
"Action": [
      "mediaconnect:action1",
      "mediaconnect:action2"
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、`List` という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "mediaconnect:List*"
```

MediaConnect アクションのリストを確認するには、IAM ユーザーガイド AWS の「Elemental MediaConnect で定義されるアクション」を参照してください。

リソース

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

MediaConnect には次の ARN があります。

```
arn:${Partition}:mediaconnect:${Region}:${Account}:entitlement:${resourceID}:
${resourceName}
arn:${Partition}:mediaconnect:${Region}:${Account}:flow:${resourceID}:${resourceName}
arn:${Partition}:mediaconnect:${Region}:${Account}:output:${resourceID}:${resourceName}
arn:${Partition}:mediaconnect:${Region}:${Account}:source:${resourceID}:${resourceName}
```

ARN の形式の詳細については、「Amazon リソースネーム (ARNs AWS 「サービス名前空間」を参照してください。

例えば、ステートメントで 1-23aBC45dEF67hiJ8-12AbC34DE5fG フローを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame"
```

特定のアカウントに属するすべてのフローを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:mediaconnect:us-east-1:111122223333:flow:*"
```

特定のリソースでは、リソースの作成など一部の MediaConnect アクションを実行できません。このような場合はワイルドカード *を使用する必要があります。

```
"Resource": "*"
```

MediaConnect API アクションの多くが複数のリソースと関連します。例えば、RemoveFlowOutput は特定のフローの出力を削除するため、IAM ユーザーはフローおよび出力のアクセス許可が必要です。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [
      "resource1",
      "resource2"
```

MediaConnect リソースタイプとその ARNs「Elemental MediaConnect で定義されるリソース AWS」を参照してください。 各リソースの ARN を指定できるアクションについては、AWS「Elemental MediaConnect で定義されるアクション」を参照してください。

条件キー

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS 「グローバル条件コンテキストキー」を参照してください。

例

MediaConnect アイデンティティベースのポリシーの例については、AWS Elemental MediaConnect アイデンティティベースのポリシーの例 を参照してください。

MediaConnect リソースベースのポリシー

AWS Elemental MediaConnect はリソースベースのポリシーをサポートしていません。

MediaConnect タグに基づく認可

AWS Elemental MediaConnect は、リソースのタグ付けやタグに基づくアクセスの制御をサポートしていません。

MediaConnect IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

MediaConnect での一時認証情報の使用

一時的な認証情報を使用して、フェデレーションでサインインする、IAM 役割を引き受ける、またはクロスアカウント役割を引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

MediaConnect は、一時認証情報の使用をサポートしています。

サービスにリンクされた役割

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

MediaConnect は、サービスリンクロールをサポートしていません。

サービス役割

この機能により、ユーザーに代わってサービスがサービス役割を引き受けることが許可されます。この役割により、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完

了することが許可されます。サービス役割はIAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者はこの役割の権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

MediaConnect はサービスロールをサポートしていません。

AWS Elemental MediaConnect アイデンティティベースのポリシーの例

デフォルトでは、IAM ユーザーおよびロールには、MediaConnect リソースを作成または変更するためのアクセス許可はありません。また、 AWS マネジメントコンソール、 AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「JSON タブでのポリシーの作成」を参照してください。

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが MediaConnect リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエ

ストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。

- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

MediaConnect コンソールの使用

AWS Elemental MediaConnect コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 AWS アカウントの MediaConnect リソースの詳細を一覧表示および表示できます。最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

これらのエンティティが MediaConnect コンソールを引き続き使用できるようにするには、エンティティに次の AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mediaconnect:*"
```

```
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteNetworkInterfacePermission"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "cloudwatch:GetMetricData"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
              }
          }
      }
  ]
}
```

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS Elemental MediaConnect リソースベースのポリシーの例

AWS Elemental MediaConnect コンソールにアクセスするには、 AWS アカウントの MediaConnect リソースの詳細を一覧表示および表示できる最小限のアクセス許可のセットが必要です。このセクションの IAM ポリシーでは、 AWS Elemental MediaConnectのリソースに対する特定のアクションを許可するポリシーの例を示しています。

のすべてのリソースへの読み取りアクセスを許可する AWS Elemental MediaConnect

AWS Elemental MediaConnect コンソールにアクセスするには、 AWS アカウントの MediaConnect リソースに対して実行できるアクションを定義するポリシーが必要です。次の IAM ポリシーで、以下のアクセス許可が提供されます。

- `mediaconnect:List*` と `mediaconnect:Describe*` のアクションのセクションは、 AWS Elemental MediaConnectで作成したすべてのリソースへの読み取り専用アクセスを許可します。
- `ec2:DescribeAvailabilityZones` アクションのセクションにより、サービスはフローがどのアベイラビリティーゾーンにあるかに関する情報を取得できます。ポリシーのこの部分は必須です。
- `cloudwatch:GetMetricData` アクションのセクションにより、サービスは Amazon CloudWatch からメトリックスを取得できます。ポリシーのこの部分は必須です。
- `iam:PassRole` アクションの セクションでは、IAM が AWS Elemental MediaConnect サービスにロールを渡して IAM と通信し、サービスに代わってロールを引き受けることを許可します。これで、その後サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。ポリシーのこの部分は必須です。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:List*",
                "mediaconnect:Describe*"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
           "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
}
```

すべての AWS Elemental MediaConnect リソースに対するすべてのアクションを許可する

のすべてのユーザーには、 リソースに対する AWS Elemental MediaConnect アクセス許可を定義するポリシー AWS Elemental MediaConnect が必要です。次の IAM ポリシーで、以下のアクセス許可が提供されます。

- `mediaconnect:*` アクションのセクションにより、 AWS Elemental MediaConnectで作成しするすべてのリソースへのすべてのアクションを許可します。

- ec2:DescribeAvailabilityZones アクションのセクションにより、サービスはフローがどのアベイラビリティーゾーンにあるかに関する情報を取得できます。ポリシーのこの部分は必須です。
- cloudwatch:GetMetricData アクションのセクションにより、サービスは Amazon CloudWatch からメトリックスを取得できます。ポリシーのこの部分は必須です。
- iam:PassRole アクションの セクションでは、IAM が AWS Elemental MediaConnect サービスにロールを渡して IAM と通信し、サービスに代わってロールを引き受けることを許可します。これで、その後サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。ポリシーのこの部分は必須です。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "mediaconnect:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ec2:DescribeAvailabilityZones"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
         {
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
```

```
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "mediaconnect.amazonaws.com"
                }
            }
        }
    ]
}
```

AWS Elemental MediaConnect に VPC 内のネットワークインターフェイスの作成と管理を許可する

この IAM ポリシーの例では、AWS Elemental MediaConnect がVPC 内にネットワークインターフェイスを作成および管理して、コンテンツが VPC から MediaConnect に流れることができるようにします。VPC をフローに接続する場合は、このポリシーを設定する必要があります。

- ec2: アクションのセクションでは、MediaConnect が VPC 内のネットワークインターフェイスを作成、読み取り、更新、削除することができます。ポリシーのこの部分は必須です。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteNetworkInterfacePermission"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Secrets Manager で MediaConnect 暗号化キーにアクセスするためのポリシー例

シークレットとして保存されている暗号化キー AWS Elemental MediaConnect の読み取りを に許可する IAM ポリシーを作成できます AWS Secrets Manager。

MediaConnect を使用して静的キー暗号化を設定するときは、 MediaConnectMediaConnect に割り当てる IAM ポリシーを作成します。このポリシーにより、MediaConnect は Secrets Manager に保存したシークレットを読み取ることができます。このポリシーの設定はお客様の判断次第です。ポリシーは、最も制限の厳しい (特定のシークレットのみへのアクセスを許可する) から、最も制限の低い (を使用して作成するシークレットへのアクセスを許可する) まで多岐にわたります AWS アカウント。ベストプラクティスとして、最も制限の厳しいポリシーを使用することをお勧めします。ただし、次の例は、さまざまな制限レベルでポリシーを設定する方法を示しています。MediaConnect はシークレットへの読み取りアクセスのみを必要とするため、すべての例に、保存する値の読み取りに必要なアクションのみが表示されます。

> **Note**
>
> Secrets Manager の次の IAM ポリシーの例はさまざまな に広く適用できますが AWS のサービス、このページでは MediaConnect のコンテキストでの使用を具体的に示しています。Secrets Manager の詳細については、 AWS Secrets Manager ドキュメントを参照してください。

トピック

- Secrets Manager で特定のシークレットへの読み取りアクセスを許可する
- Secrets Manager AWS リージョン の特定の で作成されたすべてのシークレットへの読み取りアクセスを許可する
- Secrets Manager のすべてのリソースへの読み取りアクセスを許可する

Secrets Manager で特定のシークレットへの読み取りアクセスを許可する

次の IAM ポリシーの例では、Secrets Manager で作成した特定のリソース (シークレット) への読み取りアクセスを許可します。

ARNs の############を独自の情報に置き換えます。ARNs は、MediaConnect で使用する暗号化キーを保存するシークレットを表す必要があります。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aes128-1a2b3c",
                "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aes192-4D5e6F",
                "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aes256-7g8H9i"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "secretsmanager:ListSecrets",
            "Resource": "*"
        }
    ]
}
```

Secrets Manager AWS リージョン の特定の で作成されたすべてのシークレットへの読み取りアクセスを許可する

次の IAM ポリシーは、MediaConnect に使用される暗号化キーを含め、Secrets Manager AWS リージョン の特定の で作成したすべてのシークレットへの読み取りアクセスを許可します。このポリシーは、すでに作成したリソースと、指定したリージョンで将来作成するすべてのリソースに適用さ

れます。これは、同じリージョン内で複数の暗号化された MediaConnect フローを管理する場合に役立ちます。

ARNs の############を独自の情報に置き換えます。リージョンとアカウント ID は、シークレットの保存場所を表す必要があります。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds"
            ],
            "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:*"
        },
        {
            "Effect": "Allow",
            "Action": "secretsmanager:ListSecrets",
            "Resource": "*"
        }
    ]
}
```

Secrets Manager のすべてのリソースへの読み取りアクセスを許可する

次の IAM ポリシーは、MediaConnect に使用される暗号化キーを含め、Secrets Manager で作成するすべてのリソースへの読み取りアクセスを許可します。このポリシーは、既に作成したリソースと、今後作成するすべてのリソースに適用されます。この広範なアクセスは、複数のリージョンで暗号化された MediaConnect フローを管理するときに必要になる場合があります。

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetResourcePolicy",
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret",
                "secretsmanager:ListSecretVersionIds",
                "secretsmanager:ListSecrets"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

MediaConnect フローの暗号化の設定の詳細については、このガイドの「データ保護」を参照してください。Secrets Manager の使用に関する一般的な情報については、AWS Secrets Manager 「ユーザーガイド」を参照してください。

AWS AWS Elemental MediaConnect の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

詳細については「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AWSElementalMediaConnectReadOnlyAccess

ユーザー、グループおよびロールに AWSElementalMediaConnectReadOnlyAccess をアタッチできます。

このポリシーは、ユーザーが MediaConnect ですべてのリソースを表示できるようにする読み取り専用アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- mediaconnect:ListBridges – プリンシパルが MediaConnect でブリッジのリストを表示できるようにします。これは、アカウントで使用可能なすべてのブリッジリソースを表示するために必要です。
- mediaconnect:ListEntitlements – プリンシパルが MediaConnect でエンタイトルメントのリストを表示できるようにします。これは、トランスポートストリームフローにアクセス AWS アカウント するために他の に付与されたすべてのアクセス許可を表示できるようにするために必要です。
- mediaconnect:ListFlows – プリンシパルが MediaConnect でフローのリストを表示できるようにします。これは、アカウントで使用可能なすべてのフローリソースを表示するために必要です。
- mediaconnect:ListGatewayInstances – プリンシパルが MediaConnect でゲートウェイインスタンスのリストを表示できるようにします。これは、アカウントで実行中のすべてのゲートウェイコンピューティングリソースを表示するために必要です。
- mediaconnect:ListGateways – プリンシパルが MediaConnect でゲートウェイのリストを表示できるようにします。これは、アカウントで使用可能なすべてのゲートウェイリソースを表示するために必要です。
- mediaconnect:ListOfferings – プリンシパルが MediaConnect でサービス提供のリストを表示できるようにします。これは、コミットメントを必要とする利用可能な帯域幅割引オプションを表示するために必要です。表示されるサービスは、 によって異なります AWS リージョン。
- mediaconnect:ListReservations – プリンシパルが MediaConnect で予約のリストを表示できるようにします。これは、アクティブな帯域幅コミットメントと関連する割引を確認できるようにするために必要です。
- mediaconnect:DescribeBridge – プリンシパルが MediaConnect で特定のブリッジに関する詳細情報を表示できるようにします。これは、ブリッジの設定とステータスを検査するために必要です。

- mediaconnect:DescribeFlow – プリンシパルが MediaConnect で特定のフローに関する詳細情報を表示できるようにします。これは、フローの設定とステータスを検査するために必要です。
- mediaconnect:DescribeFlowSourceMetadata – プリンシパルが MediaConnect でフローのソースに関するメタデータを表示できるようにします。これは、入力ストリームに関する技術的な詳細を表示するために必要です。
- mediaconnect:DescribeFlowSourceThumbnail – プリンシパルが MediaConnect でフローのソースのサムネイルイメージの詳細を表示できるようにします。これは、ビデオストリームのビジュアルプレビューを表示するために必要です。
- mediaconnect:DescribeGateway – プリンシパルが MediaConnect の特定のゲートウェイに関する詳細情報を表示できるようにします。これは、ゲートウェイの設定とステータスを検査するために必要です。
- mediaconnect:DescribeGatewayInstance – プリンシパルが MediaConnect の特定のゲートウェイインスタンスに関する詳細情報を表示できるようにします。これは、ゲートウェイインスタンスの設定とステータスを検査するために必要です。
- mediaconnect:DescribeOffering – プリンシパルが MediaConnect で特定のサービスに関する詳細情報を表示できるようにします。これは、帯域幅コミットメントオプションと関連する割引料金を表示するために必要です。
- mediaconnect:DescribeReservation – プリンシパルが MediaConnect で特定の予約に関する詳細情報を表示できるようにします。これは、帯域幅コミットメントとそれに関連する割引の詳細を表示するために必要です。
- mediaconnect:ListTagsForResource – プリンシパルが MediaConnect リソースに関連付けられたタグを表示できるようにします。これは、リソースの整理と分類のメタデータを表示するために必要です。

このポリシーのアクセス許可を確認するには、AWS マネージドポリシーリファレンスの[AWSElementalMediaConnectReadOnlyAccess]」を参照してください。

AWS マネージドポリシー: AWSElementalMediaConnectFullAccess

ユーザー、グループおよびロールに AWSElementalMediaConnectFullAccess をアタッチできます。

このポリシーは、MediaConnect リソースを作成、読み取り、更新、削除するアクセス許可をユーザーに付与する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `mediaconnect:*` – プリンシパルが MediaConnect ですべてのアクションを実行できるようにします。これは、管理者と他のユーザーが MediaConnect リソースを作成、読み取り、更新、削除し、ビデオトランスポートワークフローのあらゆる側面を管理できるようにするために必要です。ワイルドカード (*) アクセス許可には、フローの作成と削除、使用権限と出力の管理、ビデオ転送ワークフローの設定など、考えられるすべての MediaConnect アクションが含まれます。

このポリシーのアクセス許可を確認するには、AWS マネージドポリシーリファレンスの「AWSElementalMediaConnectFullAccess」を参照してください。

AWS マネージドポリシー: MediaConnectGatewayInstanceRolePolicy

`MediaConnectGatewayInstanceRolePolicy` ポリシーを IAM アイデンティティにアタッチできます。

このポリシーは、MediaConnect ゲートウェイインスタンスを MediaConnect ゲートウェイに登録する許可を付与します。このポリシーは、ロールにアタッチされます。ロールを引き受けるエンティティは、ゲートウェイにインスタンスを登録することができます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `mediaconnect:DiscoverGatewayPollEndpoint` – プリンシパルが指定されたゲートウェイのゲートウェイポーリングエンドポイントを見つけることを許可します。
- `mediaconnect:PollGateway` – プリンシパルが MediaConnect でゲートウェイを定期的にクエリできるようにします。これは、MediaConnect Gateway インスタンスがゲートウェイサービスから更新、設定、および指示を確認および受信できるようにするために必要です。
- `mediaconnect:SubmitGatewayStateChange` – プリンシパルが MediaConnect でステータス更新をレポートできるようにします。これは、MediaConnect Gateway インスタンスがゲートウェイサービスに運用状態、ヘルス、および設定ステータスの変更を通知するために必要です。

このポリシーのアクセス許可を確認するには、AWS マネージドポリシーリファレンスの「MediaConnectGatewayInstanceRolePolicy」を参照してください。

AWS マネージドポリシー: AWS MediaConnectServicePolicy

AWS MediaConnectServicePolicy を IAM エンティティにアタッチすることはできません。このポリシーは、MediaConnect がユーザーに代わってアクションを実行できるようにするサービスリンクロールに関連付けられています。詳細については、「サービスリンクロールの使用」を参照してください。

このポリシーは、AWS ServiceRoleForMediaConnect サービスリンクロールにアタッチされます。このポリシーにより、サービスリンクロールがユーザーに代わって Amazon ECS リソースを管理できるようになります。AWS Elemental MediaConnect Gateway は、AWS Elemental MediaConnect Gateway のオンプレミス実装の基盤として Amazon ECS を使用しており、MediaConnect には、必要に応じて Amazon ECS リソースを作成、更新、削除する機能が必要です。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

> **Note**
>
> これらのアクセス許可はすべて、 条件ブロックMediaConnectGatewayから で始まる名前の ECS クラスターに制限されます。

- ecs:UpdateService – プリンシパルが既存の ECS サービスを変更できるようにします。これは、MediaConnect が ECS で実行されている MediaConnect Gateway コンポーネントのサービス設定を更新できるようにするために必要です。
- ecs:DeleteService – プリンシパルが ECS サービスを削除できるようにします。これは、MediaConnect が不要になったサービスをクリーンアップできるようにするために必要です。
- ecs:CreateService – プリンシパルが新しい ECS サービスを確立できるようにします。これは、MediaConnect が Gateway 実装用の新しいサービスコンポーネントをセットアップできるようにするために必要です。
- ecs:DescribeServices – プリンシパルが ECS サービスの詳細を表示できるようにします。これは、MediaConnect がサービスの状態を監視および管理できるようにするために必要です。
- ecs:PutAttributes – プリンシパルが ECS リソースに属性を追加できるようにします。これは、MediaConnect が必要なメタデータを適用してリソースを設定できるようにするために必要です。

- ecs:DeleteAttributes – プリンシパルが ECS リソースから属性を削除できるようにします。これは、MediaConnect が不要になったメタデータをクリーンアップできるようにするために必要です。
- ecs:RunTask – プリンシパルが ECS で新しいタスクを開始できるようにします。これは、MediaConnect が必要に応じて新しい Gateway コンポーネントを起動できるようにするために必要です。
- ecs:ListTasks – プリンシパルが ECS ですべてのタスクを表示できるようにします。これは、MediaConnect が実行中のタスクをモニタリングおよび管理できるようにするために必要です。
- ecs:StartTask – プリンシパルが ECS で特定のタスクを開始できるようにします。これは、MediaConnect が特定のゲートウェイコンポーネントを起動できるようにするために必要です。
- ecs:StopTask – プリンシパルが ECS で実行中のタスクを終了できるようにします。これは、MediaConnect が必要に応じて Gateway コンポーネントを停止できるようにするために必要です。
- ecs:DescribeTasks – プリンシパルが ECS タスクの詳細を表示できるようにします。これは、MediaConnect が実行中のタスクのステータスをモニタリングできるようにするために必要です。
- ecs:DescribeContainerInstances – プリンシパルが ECS コンテナインスタンスの詳細を表示できるようにします。これは、MediaConnect が Gateway コンポーネントのヘルスとステータスをモニタリングできるようにするために必要です。
- ecs:UpdateContainerInstancesState – プリンシパルがコンテナインスタンスの状態を変更できるようにします。これは、MediaConnect がコンテナインスタンスのライフサイクルを管理できるようにするために必要です。

このポリシーのアクセス許可を確認するには、AWS マネージドポリシーリファレンスの「AWSMediaConnectServicePolicy」を参照してください。

AWS 管理ポリシーに対する MediaConnect の更新

このサービスがこれらの変更の追跡を開始してからの MediaConnect の AWS 管理ポリシーの更新に関する詳細を表示します。このページの変更に関する自動通知については、「ドキュメントの履歴」ページの RSS フィードをサブスクライブしてください。

変更	説明	日付
MediaConnect 管理ポリシー AWSElementalMediaConnectReadOnlyAccess が追加されました。	このポリシーは、MediaConnect リソースへの読み取り専用アクセスを提供します。	2025 年 2 月 12 日
MediaConnect 管理ポリシー AWSElementalMediaConnectFullAccess が追加されました。	このポリシーは、MediaConnect リソースへのフルアクセスを提供します。	2025 年 2 月 12 日
MediaConnect マネージドポリシー MediaConnectGatewayInstanceRolePolicy が追加されました。	このポリシーは、MediaConnect ゲートウェイインスタンスを MediaConnect ゲートウェイに登録する許可を付与します。	2023 年 4 月 12 日
MediaConnect マネージドポリシー AWSMediaConnectServicePolicy が追加されました。	このポリシーは、サービスリンクロールによって使用され、MediaConnect で使用される AWS サービスとリソースにアクセスするためのアクセス許可を付与します。	2023 年 4 月 12 日
MediaConnect が変更の追跡を開始しました	MediaConnect は AWS 、管理ポリシーの変更の追跡を開始しました。	2023 年 4 月 12 日

MediaConnect 向けのサービスリンクロールの使用

AWS Elemental MediaConnect は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスリンクロールは、MediaConnect に直接リンクされた一意のタイ

プの IAM ロールです。サービスにリンクされたロールは MediaConnect によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスリンクロールを使用することで、必要なアクセス許可を手動で追加する必要がなくなるため、MediaConnect の設定が簡単になります。MediaConnect は、サービスリンクロールのアクセス許可を定義します。特に定義されている場合を除き、MediaConnect のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、最初に関連リソースを削除する必要があります。これにより、リソースへのアクセス許可が意図せず削除されることが防止されるので、MediaConnect リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスの詳細については、AWS 「IAM と連携するサービス」を参照し、「サービスにリンクされたロール」列で「はい」を持つサービスを探します。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[Yes] (はい) リンクを選択します。

MediaConnect のサービスリンクロール許可

MediaConnect は、AWSServiceRoleForMediaConnect という名前のサービスリンクロールを使用します。これは、MediaConnect によって使用または管理される AWS のサービスとリソースへのアクセスを可能にする、デフォルトのService-Linked Role (サービスリンクロール) です。

サービスリンクロール AWSServiceRoleForECS は、次のサービスを信頼してロールを引き受けます。

- `MediaConnect`

MediaConnectServiceRolePolicy というロールアクセス許可ポリシーは、MediaConnect に、指定されたリソースで次のアクションを完了することを許可します。

- アクション: リソース `arn:aws:ecs:*:*:*` での `ecs:CreateCluster, ecs:RegisterTaskDefinition, ecs:DescribeTaskDefinition, ecs:ListAttributes, ecs:UpdateContainerInstancesState, ecs:DeregisterContainerInstance`
- アクション: リソース `arn:aws:ecs:*:*:cluster/MediaConnect` での `ecs:UpdateCluster, ecs:UpdateClusterSettings, ecs:DescribeClusters`

- アクション: 条件が `StringLike: {ecs:Cluster: arn:aws:ecs:*:*:cluster/MediaConnect}` であるリソース `ecs:CreateService, ecs:UpdateService, ecs:RunTask, ecs:StartTask, ecs:StopTask, ecs:ExecuteCommand, ecs:PutAttributes, ecs:DeleteAttributes, ecs:DescribeServices, ecs:DescribeTasks, ecs:ListTasks` での `arn:aws:ecs:*:*:*`

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス許可を設定する必要があります。詳細についてはIAM ユーザーガイド の「サービスにリンクされた役割のアクセス許可」を参照してください。

MediaConnect のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。 AWS マネジメントコンソール、、AWS CLIまたは AWS API で関連付けられた MediaConnect リソースを作成すると、MediaConnect によってサービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスリンク役割はこの役割でサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。MediaConnect がサービスリンクロールのサポートを開始した 2023 年 3 月 1 日より前にこのサービスを使用していた場合、MediaConnect によってアカウントに AWSServiceRoleForMediaConnect ロールが作成されています。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。関連付けられた MediaConnect リソースを作成すると、MediaConnect によってサービスリンクロールが再び作成されます。

MediaConnect ユースケースでサービスリンクロールを作成する場合は、IAM コンソールも使用できます。 AWS CLI または AWS API で、サービス名を使用して`MediaConnect`サービスにリンクされたロールを作成します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの作成」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

MediaConnect でのサービスリンクロールの編集

MediaConnect では、サービスリンクロール AWSServiceRoleForMediaConnect を編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

MediaConnect のサービスリンクロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースの削除を試みた際に、このロールが MediaConnect のサービスで使用されている場合、削除処理が失敗することがあります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForMediaConnect が使用している MediaConnect リソースを削除するには

1. すべてのゲートウェイのブリッジをすべて削除します。
2. すべてのゲートウェイのすべてのインスタンスを登録解除します。
3. すべてのゲートウェイを削除します。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、 AWS CLI、または AWS API を使用して、AWSServiceRoleForMediaConnect サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

MediaConnect のサービスリンクロールをサポートするリージョン

MediaConnect は、サービスが利用可能なすべてのリージョンでサービスリンクロールの使用をサポートします。詳細については、「MediaConnect のリージョンとエンドポイント」を参照してください。

AWS Elemental MediaConnect を信頼されたサービスとしてセットアップする

AWS Identity and Access Management (IAM) を使用して、ユーザーとアプリケーションがアクセスできる AWS リソースを制御できます。これには、AWS Elemental MediaConnect がアカウントに代わって他のサービスと通信できるようにするためのアクセス許可の設定が含まれます。AWS Elemental MediaConnect を信頼できるエンティティとしてセットアップするには、次のステップを実行する必要があります。

ステップ 1. どのアクションを許可するかを管理する IAM ポリシーを作成します。

ステップ 2: 信頼できる関係を持つ IAM ロールを作成し、前のステップで作成したポリシーをアタッチします。

ステップ 1: 特定のアクションを許可する IAM ポリシーを作成します

このステップでは、許可するアクションを制御する IAM ポリシーを作成します。

IAM ポリシーを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、ポリシー を選択してください。
3. ポリシーの作成 を選択し、JSON タブを選択します。
4. JSON 形式を使用するポリシーを入力します。 の例については、次を参照してください。
   - VPC に接続するためのポリシーの例
   - のシークレットのポリシー例 AWS Secrets Manager
5. [ポリシーの確認] を選択します。
6. [名前] に IAM ポリシーの名前を入力します。
7. [Create policy] (ポリシーの作成) を選択します。

ステップ 2: 信頼できる関係を持つ IAM ロールを作成する

ステップ 1 では、許可するアクションを管理する IAM ポリシーを作成しました。この手順では、IAM ロールを作成し、このポリシーをロールに割り当てます。次いで、AWS Elemental MediaConnect を、ロールを引き受け可能な信頼できるエンティティとして定義します。

信頼関係のあるロールを作成するには

1. IAM コンソールのナビゲーションペインで [ロール] を選択します。
2. [Role] (ロール) ページで、[Create role] (ロールの作成) を選択します。
3. [ロールを作成] ページの 信頼されたエンティティのタイプを選択 セクションで、[AWS サービス] (デフォルト)を選択します 。
4. [Choose the service that will use this role] (このロールを使用するサービスを選択) で、[EC2] を選択します。

   MediaConnect は現在リストに含まれていないため、EC2 を選択します。EC2 を選択すると、ロールを作成できます。後の手順で、このロールを変更し、EC2 を MediaConnect に置き換えます。
5. [Next: Permissions] (次のステップ: 許可) を選択します。
6. [許可ポリシーをアタッチ] には、ステップ 1 で作成したポリシーの名前を入力してください。
7. ポリシー名の横にあるチェックボックスをオンにして、次へ: タグを選択します。
8. (オプション) タグをキーバリューペアとしてアタッチして、メタデータをユーザーに追加します。IAM でのタグの使用の詳細については、IAM ユーザーガイドの「IAM リソースのタグ付け」を参照してください。
9. [Next: Review] を選択します。
10. [Role name] (ロール名) に名前を入力します。名前 `MediaConnectAccessRole` は予約されているため、使用できません。代わりに、`MediaConnect` を含み、このロールの目的を説明する名前を使用します。
11. ロールの説明では、デフォルトのテキストをこのロールの目的を覚えるのに役立つ説明に置き換えます。
12. [ロールの作成] を選択してください。
13. ページの上部に表示される確認メッセージで、[ロールを表示] を選択して作成したロールの名前を選択します。
14. [信頼関係] タブを選択し、続いて [信頼ポリシーの編集] を選択します。
15. [信頼ポリシーの編集] ウィンドウで、JSON を次のように変更します。

    - [サービス] で、`ec2.amazonaws.com` を `mediaconnect.amazonaws.com` に変更します。
    - セキュリティを強化するには、信頼ポリシーに特定の条件を定義します。これにより、MediaConnect はアカウント内のリソースのみを使用するように制限されます。これを行うには、[アカウント ID]、[フロー ARN]、またはその両方などのグローバル条件を使用しま

す。以下の信頼ポリシーの例を参照してください。グローバル条件によるセキュリティ上の利点の詳細については、「サービス間での混乱した代理問題の防止」を参照してください。

> **Note**
>
> 次の例では、[アカウント ID] と [フロー ARN] 条件の両方を使用しています。両方の条件を使用しないと、ポリシーの見え方が変わります。フローの完全な ARN が不明な場合や、複数のフローを指定する場合には、グローバルコンテキスト条件キー `aws:SourceArn` で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば、`arn:aws:mediaconnect:*:111122223333:*`。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "mediaconnect.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:mediaconnect:us-
west-2:111122223333:flow:*:flow-name"
                }
            }
        }
    ]
}
```

16. [ポリシーの更新] を選択してください。
17. [Summary] (概要) ページで、[Role ARN] (ロール ARN) の値をメモします。以下のような形式です：`arn:aws:iam::111122223333:role/MediaConnectASM`

サービス間での不分別な代理処理の防止

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、 AWS では、アカウントのリソースへのアクセス権が付与されたサービスプリンシパルで、すべてのサービスのデータを保護するために役立つツールを提供しています。

フローの aws:SourceArn およびリソースポリシー内の aws:SourceAccount グローバル条件コンテキストキーを使用して、AWS Elemental MediaConnect がそのリソースに対して別のサービスに付与する許可を制限することをお勧めします。クロスサービスのアクセスにリソースを 1 つだけ関連付ける場合は、フローの aws:SourceArn を使用します。クロスサービスが使用できるように、アカウント内の任意のリソースを関連付ける場合は、aws:SourceAccount を使用します。

混乱した代理問題から保護するための最も効果的な方法は、フローの完全な ARN を指定しながら、aws:SourceArn グローバル条件コンテキストキーを使用することです。フローの完全な ARN が不明な場合や、複数のフローを指定する場合には、グローバルコンテキスト条件キー aws:SourceArn で、ARN の未知部分を示すためにワイルドカード文字 (*) を使用します。例えば、arn:aws:mediaconnect:*:*111122223333*:*。

以下は、混乱した使節の問題を防止するために、MediaConnect で aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用する方法の例です。

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "mediaconnect.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:mediaconnect:us-
west-2:111122223333:flow:1-ABCDEFGHJxyzMNoP-a1234bc12345:flow-name"
                }
            }
        }
    ]
}
```

Elemental MediaConnect AWS のアイデンティティとアクセスのトラブルシューティング

次の情報は、MediaConnect と IAM の使用時に発生する可能性がある、一般的な問題の診断や修復に役立ちます。

トピック

- MediaConnect でアクションを実行する権限がない場合
- 自分の AWS アカウント以外のユーザーに MediaConnect リソースへのアクセスを許可したい

MediaConnect でアクションを実行する権限がない場合

でアクションを実行する権限がないと AWS マネジメントコンソール 通知された場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

次の例のエラーは、mateojackson ユーザーがコンソールを使用してフローの詳細を表示しようとしたが、mediaconnect:DescribeFlow 権限を持っていない場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 mediaconnect:DescribeFlow on resource: myExampleFlow
```

この場合、Mateo は、mediaconnect:DescribeFlow アクションを使用して myExampleFlow リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

自分の AWS アカウント以外のユーザーに MediaConnect リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- MediaConnect がこれらの機能をサポートしているかどうかを確認するには、「Elemental MediaConnect AWS と IAM の連携方法」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

ログ記録とモニタリング

このセクションでは、セキュリティ上の目的で AWS Elemental MediaConnect 内でログ記録およびモニタリングを行うためのオプションについての概要を説明します。MediaConnect でのログ記録およびモニタリングの詳細については、「モニタリングとタグ付け」を参照してください。

モニタリングは、 および AWS Elemental MediaConnect AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、 AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。 には、MediaConnect リソースをモニタリングし、潜在的なインシデントに対応するための複数のツール AWS が用意されています。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用して、指定した期間にわたって 1 つのメトリクスを確認します。メトリクスが特定のしきい値を超えると、Amazon SNS トピックまたは AWS Auto Scaling (自動スケーリング) ポリシーに通知が送信されます。CloudWatch アラームは、特定の状態にあるという理由ではアクションを呼び出しません。その代わり、状態が変更され、指定期間にわたって維持される必要があります。詳細については、「CloudWatch メトリクスを使用したモニタリング」を参照してください。

AWS CloudTrail ログ

CloudTrail は、 のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します AWS Elemental MediaConnect。CloudTrail で収集された情報を使用して、MediaConnect に送られたリクエスト、リクエスト発行元の IP アドレス、リクエスト発行者、リクエストの発行日時、その他の詳細を確認できます。詳細については、「AWS CloudTrail による API コールのログ記録」を参照してください。

AWS Trusted Advisor

Trusted Advisor は、数十万の AWS 顧客へのサービス提供から学んだベストプラクティスを活用します。 は AWS 環境 Trusted Advisor を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があれば、レコメンデーションを行います。すべての AWS お客様は、5 つの Trusted Advisor チェックにアクセスできます。ビジネスまたはエンタープライズサポートプランをご利用のお客様は、すべての Trusted Advisor チェックを表示できます。

詳細については、「AWS Trusted Advisor」を参照してください。

のコンプライアンス検証 AWS Elemental MediaConnect

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス「コンプライアンスプログラムによる範囲内」を参照して、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべての AWS のサービス が HIPAA の対象となるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティコントロールを保護および AWS のサービス マッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub CSPM – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 不審なアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで AWS アカウント、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS Elemental MediaConnect

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS Elemental MediaConnect

マネージドサービスである AWS Elemental MediaConnect は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で MediaConnect にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

MediaConnect インターフェイス VPC エンドポイント (AWS PrivateLink)

インターフェイス VPC エンドポイントを使用すると、Amazon ネットワーク内の VPC および MediaConnect 間のすべての MediaConnect API リクエストのトラフィックを維持できます。これにより、VPC のセキュリティが向上します。インターフェイス VPC エンドポイントでは、インターネットゲートウェイ、NAT デバイス、または仮想プライベートゲートウェイも必要ありません。VPC エンドポイントは AWS PrivateLink、プライベート IP アドレスを使用して MediaConnect APIs にプライベートにアクセスするために使用できるテクノロジーである を利用しています。

AWS PrivateLink および VPC エンドポイントの詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイント」を参照してください。

MediaConnect VPC エンドポイントに関する考慮事項

MediaConnect のインターフェイスエンドポイントを設定する前に、Amazon VPC ユーザーガイドの「インターフェイスエンドポイントのプロパティと制限」を確認してください。

- 現在、VPC エンドポイントはクロスリージョンリクエストをサポートしていません。必ず、MediaConnect と通信するリージョンと同じリージョンにエンドポイントを作成してください。
- VPC エンドポイントでは、Amazon Route 53 を介して Amazon 提供の DNS のみがサポートされています。独自の DNS を使用したい場合は、条件付き DNS 転送を使用できます。詳細については、Amazon VPC ユーザーガイドのDHCP Options Setsを参照してください。
- VPCエンドポイントにアタッチされたセキュリティグループでは、VPCのプライベートサブネットから、ポート 443 で着信接続を許可する必要があります。

MediaConnect 用の VPC エンドポイントの作成

MediaConnect のインターフェイスエンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。Amazon VPC ユーザーガイドの「インターフェイスエンドポイントの作成」で説明されている手順に従ってください。

MediaConnect 用の VPC エンドポイントへのアクセス制御

VPC エンドポイントには、MediaConnect へのアクセスを制御するエンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル。

- 実行可能なアクション。
- アクションを実行できるリソース。

詳細については、「Amazon VPC ユーザーガイド」の「VPC エンドポイントでサービスへのアクセスを制御する」を参照してください。

例: アクション用の VPC エンドポイントポリシー

以下は、MediaConnect 用のエンドポイントポリシーの例です。エンドポイントにアタッチされると、このポリシーは、すべてのリソースですべてのプリンシパルに、リストされている MediaConnect アクションへのアクセス権を付与します。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "mediaconnect:action-1",
            "mediaconnect:action-2",
            "mediaconnect:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Elemental MediaConnect でのモニタリングとタグ付け

モニタリングは、AWS Elemental MediaConnect およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持するための重要な部分です。AWS には、MediaConnect を監視したり、問題が発生したときに報告したり、必要に応じて自動アクションを実行したりするために以下のモニタリングツールが用意されています。

- AWS CloudTrail は、AWSアカウントにより、またはそのアカウントに代わって行われた API コールや関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrailユーザーガイドを参照してください。
- Amazon CloudWatch Events は、AWS リソースの変更を示すシステムイベントをほぼリアルタイムのストリーミングとして提供します。CloudWatch Events で自動イベント駆動型コンピューティングを有効にすると、特定のイベントをモニタリングするルールを記述し、そのイベントが発生したときに他の AWS のサービスで自動アクションをトリガーできます。詳細については、「Amazon CloudWatch Events ユーザーガイド」を参照してください。
- Amazon CloudWatch は、AWS のリソースおよび AWS で実行しているアプリケーションをリアルタイムでモニタリングします。メトリクスを収集および追跡し、カスタマイズされたダッシュボードを作成し、指定されたメトリックが指定したしきい値に達したときに通知またはアクションを実行するアラームを設定できます。例えば、AWS Elemental MediaConnect フローでドロップされたパケットと回復されなかったパケットの数を CloudWatch に追跡させ、それらの値が特定の数を超えたときに自動的に通知させることができます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

Amazon CloudWatch メトリクスを使用し、AWS Elemental MediaConnect をモニタリングする

raw データを収集し、ほぼリアルタイムで、読み取り可能なメトリクスに処理するCloudWatch を使用して AWS Elemental MediaConnect をモニタリングできます。これらの統計は 15 か月間保持されるため、履歴情報にアクセスし、ウェブアプリケーションやサービスの動作をより的確に把握できます。ほとんどの MediaConnect メトリクスには、最短 1 秒でアクセスできます。また、特定のしきい値をモニタリングするアラームを設定し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

フローの CloudWatch メトリクスを MediaConnect コンソールで直接表示できます。コンソールでは、最短 1 分から最長 30 分の時間でこれらのメトリクスを表示できます。

> **Note**
>
> MediaConnect ゲートウェイのメトリクスは、高解像度時間 (1 秒) では利用できません。最低 1 分以上の時間を選択する必要があります。

メトリクスの定義

AWS Elemental MediaConnectは、メトリクスの基礎となるデータを収集します。これらのデータポイントは毎秒収集され、すぐに Amazon CloudWatch に送信されます。CloudWatch を使用して、これらのデータポイントのメトリクスを生成できます。

メトリクスとは、集計 (統計)が適用され、期間と時間範囲が設定されたデータポイントを収集したものです。例えば、ドロップパケット数のメトリクスを 10 分 (時間範囲) にわたる 1 分間の平均 (統計) としてリクエストできます。このリクエストの結果は 10 メトリクスです (範囲を期間で割ると 10 であるため)。

[Period] (期間)

ほとんどの MediaConnect メトリクスには高解像度時間があります。つまり、最小時間は 1 秒です。MediaConnect ゲートウェイのメトリクスは、高解像度時間で利用できない唯一のメトリクスです。

[Time range] (時間範囲)

各期間には最大時間範囲があります。例えば、時間範囲に 3 時間を指定した場合、10 秒間のメトリクスを取得することはできません。

[Period] (期間)	最大時間範囲
1 秒	最低 3 時間
5 秒	
10 秒	

[Period] (期間)	最大時間範囲
30 秒	
60 秒	過去 360 時間 (15 日間)
300 秒 (5 分)	過去 1512 時間 (63 日間)
900 秒 (15 分)	
3600 秒 (1 時間) またはそれ以上	過去 455 日 (15 か月)

期間には最低時間範囲はありません。しかし、期間が短いと、適用する統計が意味をなさなくなる時点があります。例えば、期間を 1 秒に設定するとします。これは、CloudWatch が 1 つのデータポイントを取得することを意味します。1 つのデータポイントの平均値、最小値、最大値を取得することはできません。ただし、だからといって、メトリクスが無意味であるわけではありません。その代わりに、メトリクスは統計情報のない未加工のデータポイントになります。

最大ストレージ時間

メトリクスは、最近 15 か月間使用できます。希望する期間を必ず指定するようにしてください。

メトリクスの表示

一部のメトリクスは MediaConnect コンソールで表示できます。Amazon CloudWatch コンソールでメトリクスを表示できます。CLI、REST API、または任意の AWS SDK を使用してメトリクスを取得することもできます。

CloudWatch コンソールでは、メトリクスの最小リフレッシュレートは 30 秒です。

MediaConnect コンソールでメトリクスを表示するには

一部のメトリクスは MediaConnect コンソールで表示できます。現在のメトリクスを、1 時間から 1 週間前に遡って表示することができます。(他のメトリクスや、過去のメトリクスを表示するには、CloudWatch コンソールを使用する必要があります)。

1. MediaConnect コンソール (https://console.aws.amazon.com/mediapackage/) を開きます。
2. ナビゲーションペインで、[Flows] (フロー) を選択します。フロー ページで、目的のフローを選択します。[詳細] ページが表示されます。

3. 「ヘルス」タブを選択します。MediaConnect がこのタブでサポートするメトリクスが表示されます。
4. 期間と時間範囲を選択します。例えば、「過去 1 日 (5 分間)」などです。

CloudWatch コンソールを使用してメトリクスを表示するには

CloudWatch コンソールでは、任意の期間の MediaConnect のすべてのメトリクス (現在または過去のメトリクス) を表示できます。CloudWatch コンソールでメトリクスを表示するには料金がかかります。

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[メトリクス] 、[すべてのメトリクス] の順に選択します。ページの下半分の [ブラウズ] タブでは、名前の付いたカードが表示されます。

   全く初めてであり、いずれのサービスでもメトリクスを作成するアクションを実行したことがない場合はAWS、カードは表示されません。
3. AWS/MediaConnect という名前のカードを選択します。

   このカードは、現在 CloudWatch 用に選択されているAWSのリージョンで、最近 15 か月間に少なくとも 1 つのフローを開始した場合にのみ表示されます。MediaConnect フローを開始したことがない場合は、このカードは表示されません。その場合は、フローを作成し、その後に開始してこの手順に戻ってください。

   (ページのカスタム名前空間セクションに MediaConnect という名前のカードが表示される場合があります。このカードは、MediaConnect メトリクスの古いネームスペース用です。 この 2 つの名前スペースは 2022 年 9 月に互いに重複しているため、このカードを選択してもメリットはありません。 いつも、必ず AWS/MediaConnect を選択してください。)
4. ページの下半分にある [ブラウズ] タブにディメンションが表示されるようになりました。メトリクスディメンションを選択します。例えば、[フロー ARN] を選択します。

   ブラウズ タブに、選択したディメンション (例、フロー ARN) を示す 1 つの列と、すべてのメトリクスを表示する 1 つの列がある表が表示されるようになりました。テーブルをソートできます。
5. 1 つまたは複数の行を選択します。行を選択すると、ページの上半分のグラフにその行が表示されます。
6. ページの下半分にある [グラフメトリクス] タブを選択します。
7. タブの右側の選択肢で、「統計」と「期間」を指定します。

期間を選択すると、グラフが更新され、その期間の最大時間範囲が表示されます。ここで左側のグラフが空になったら、グラフの右上にある選択肢でタイムラインを調整できます。スペースが完全に埋まるように、小さい値の数字を選択してください。たとえば、1w を 1dに変更します。

AWS CLI を使ってメトリクスを表示するには

- コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/MediaConnect"
```

フローの状態を監視するための AWS Elemental MediaConnect メトリクス

AWS Elemental MediaConnect は CloudWatch にメトリクスを送信します。特定のメトリクスを確認してフローの状態を評価できます。フローに問題がある場合、これらのメトリクスは問題の原因を突き止めるのに役立ちます。各メトリクスの詳細については、このセクションの表を参照してください。

ソースの詳細については、「ソースの状態を監視するメトリクス」をご参照ください。

> **Note**
>
> MediaConnect によって追跡されるメトリクスは、TR 101 290 仕様で定義されている基準に準拠しています。

トピック

フローメトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信するネットワークのメトリクスが記載されています。

メトリクス	説明
ARQRecovered	自動再送要求 (ARQ) によって回復された、ドロップされたバケットの数。このメトリクスは、エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。複数のソースがあるフローでは、SourceARQRecovered メトリクスを使用して各ソースのデータを表示します。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
ARQRequests	自動再送要求 (ARQ) を通じて要求され、受信された再送信パケットの数。このメトリクスは、エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。複数のソースがあるフローでは、SourceARQRequests メトリクスを使用して各ソースのデータを表示します。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
BitRate	受信 (ソース) ビデオのビットレート。 単位: ビット/秒 (b/s) 有効なディメンション: • フロー ARN • アベイラビリティーゾーン

メトリクス	説明
	• すべてのフロー
Connected	リソースのステータス。値 1 は、ソースが接続されたことを示します。値 0 (ゼロ) は、ソースが切断されたことを示します。このメトリクスは、Zixi、SRT、富士通、または RIST プロトコルを使用するソースにのみ適用されます。 単位: なし 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
Disconnections	ソースステータスが接続から切断に変わった回数。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
DroppedPackets	転送中に失われたパケット数。この値は、エラー修正が行われる前に測定されます。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
FECPackets	前方誤り訂正 (FEC) を使用して送信され、受信されたパケットの数。このメトリクスクは、RTP-FEC、Zixi、または富士通のプロトコルを使用するソースが 1 つあるフローにのみ適用されます。エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。複数のソースがあるフローでは、SourceFecPackets メトリクスを使用して各ソースのデータを表示します。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
FECRecovered	前方誤り訂正 (FEC) を使用して送信され、転送中に失われたパケットおよび回復されたパケットの数。このメトリクスクは、RTP-FEC、Zixi、または富士通のプロトコルを使用するソースが 1 つあるフローにのみ適用されます。エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。複数のソースがあるフローでは、SourceFecRecovered メトリクスを使用して各ソースのデータを表示します。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
MergeActive	フロー上のすべてのソースのマージステータス。値 1 は、すべてのソースがマージされたことを示します。値 0 (ゼロ) は、少なくとも 1 つのソースが 2022-7 と能動的にマージされていないことを示します。 単位: なし 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
MergeLatency	SourceMergeLatency の最大値。 単位: ミリ秒 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
NotRecoveredPackets	転送中に失われ、エラー修正によって回復されなかったパケットの数。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
OverflowPackets	ビデオが使用許容量よりも多くのバッファを必要としたために、転送中に失われたパケットの数。このメトリクスは、エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
PacketLossPercent	回復したにも関わらず、転送中に失われたパケットの割合。 単位: パーセント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
RecoveredPackets	転送中に失われたが、回復したパケット数。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
RoundTripTime	ソースがシグナルを送信し、AWS Elemental MediaConnect からの確認を受信するまでにかかる時間。このメトリクスは、エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。複数のソースがあるフローでは、SourceRoundTripTime メトリクスを使用して各ソースのデータを表示します。 単位: ミリ秒 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
TotalPackets	受信されるパケットの総数。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
FailoverSwitches	ソースフェイルオーバーにフェイルオーバーモードを使用する場合に、フローがソース間を行き来する合計回数。

TR 101 290 プライオリティ 1 メトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信する TR 101 290 プライオリティ 1 のメトリクスが記載されています。

メトリクス	説明
ContinuityCounter	連続エラーが発生した回数。このエラーは、パケットの順序が正しくないか、パケットが失われたことを示しています。

メトリクス	説明
	単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
PATError	プログラムアソシエーションテーブル (PAT) エラーが発生した回数。このエラーは PAT が欠落していることを示しています。PAT はトランスポートストリーム (TS) で利用可能なプログラムを一覧表示し、プログラムマップテーブル (PMT) を示します。デコーダーがその役割を果たすには PAT が必要です。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
PIDError	パケット識別子 (PID) エラーが発生した回数。このエラーは、PID に関連するデータストリームが欠落していることを示します。PID は、ビデオ、オーディオ、およびデータストリームの場所を提供する識別子です。このエラーは、トランスポートストリームを多重化してから再度多重化した後に発生する可能性があります。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
PMTError	プログラムマップテーブル (PMT) エラーが発生した回数。このエラーは、PMT が少なくとも 500 ミリ秒 (ms) ごとに受信されない場合に発生します。各 PMT には、デコーダーがデータを再構成するのに役立つ PID のリストが含まれています。デコーダーがその役割を果たすには PMT が必要です。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
TSByteError	トランスポートストリームのバイトエラーが発生した回数。このエラーは、同期バイトが規定のバイト数を超えて表示されなかったことを示しています。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
TSSyncLoss	TS 同期喪失エラーが発生した回数。このエラーは、TS バイトエラーが 2 回以上連続した後に発生します。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

TR 101 290 プライオリティ 2 メトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信する TR 101 290 プライオリティ 2 のメトリクスが記載されています。

メトリクス	説明
CATError	条件付きアクセステーブル (CAT) エラーが発生した回数。このエラーは、CAT が存在しないことを示しています。CAT は、統合レシーバーデコーダー (IRD) に、使用中の条件付きアクセス (CA) システムの管理メッセージの保存先を伝えます。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
CRCError	巡回冗長検査 (CRC) エラーが発生した回数。このエラーは、CRC が、データが破損していると判断した場合に発生します。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
PCRAccuracyError	プログラムクロックレジスター(PCR) の精度エラーが発生した回数。このエラーは、送信された PCR の値が予想値と 500 ナノ秒 (ns) 以上異なる場合に発生します。ストリームがエンコードされると、エンコーダーはエンコーダーのプログラムクロックに定期的に PCR 値を割り当てます。デコーダーはこれらの値に基づいてストリームの同期が保たれるようにします。 単位はカウント

メトリクス	説明
	有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
PCRError	PCR エラーが発生した回数。このエラーは、PCR 値が十分な頻度で送信されない場合に発生します。このサービスは、ローカル 27 MHz のシステムクロックをリセットするために、一貫性のある頻繁な PCR に依存しています。このエラーは間隔が 100 ミリ秒 (ms) を超えると発生しますが、ベストプラクティスでは、PCR は少なくとも 40 ミリ秒ごとに受信するようになっています。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー
PTSError	プレゼンテーションタイムスタンプ (PTS) エラーが発生した回数。このエラーは、少なくとも 700 ミリ秒ごとにプレゼンテーションタイムスタンプ (PTS) が受信されない場合に発生します。このエラーは、PTS の送信頻度が低いか、まったく送信されない場合に発生する可能性があります。このエラーの最も一般的な原因は、トランスポートストリーム (TS) がスクランブルされることです。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
TransportError	プライマリトランスポートエラーが発生した回数。このエラーは、TS パケットが使用できないことを示しています。このエラーが発生した場合は、このパケットのその他の TR 101 290 エラーをすべて無視してください。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メンテナンスメトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信するメトリクスが記載されています。

メトリクス	説明
MaintenanceScheduled	メンテナンスはフローに合わせて予定されています。 単位はカウント 有効なディメンション: • フロー ARN • すべてのフロー
MaintenanceRescheduled	MediaConnect は、以前に予定されていた日時にメンテナンスを行うことができません。このフローのメンテナンスのために、MediaConnect によって新しい日付と時刻が自動的に割り当てられました。 単位はカウント 有効なディメンション: • フロー ARN

メトリクス	説明
	• すべてのフロー
MaintenanceCanceled	このフローのメンテナンスは MediaConnect によってキャンセルされます。 単位はカウント 有効なディメンション: • フロー ARN • すべてのフロー
MaintenanceStarted	このフローのメンテナンスが開始され、現在進行中です。 単位はカウント 有効なディメンション: • フロー ARN • すべてのフロー
MaintenanceSucceeded	このフローのメンテナンスは正常に完了しました。 単位はカウント 有効なディメンション: • フロー ARN • すべてのフロー
MaintenanceFailed	このフローのメンテナンスは正常に完了しませんでした。 単位はカウント 有効なディメンション: • フロー ARN • すべてのフロー

ソースの状態を監視するための AWS Elemental MediaConnect メトリクス

AWS Elemental MediaConnect は CloudWatch にメトリクスを送信します。特定のメトリクスを確認して、フローのソースの状態を評価できます。フローに問題がある場合、これらのメトリクスは問題の原因がソースにあるかどうかを判断するのに役立ちます。各メトリクスの詳細については、このセクションの表を参照してください。

メトリクスの詳細については、「フローの状態を監視するメトリクス」を参照してください。

> **Note**
>
> MediaConnect によって追跡されるメトリクスは、TR 101 290 仕様で定義されている基準に準拠しています。

トピック

ソースメトリクス

次の表に、AWS Elemental MediaConnect が CloudWatch に送信するメトリクスが記載されています。

メトリクス	説明
`SourceARQ Recovered`	自動再送要求 (ARQ) によって回復された、ドロップされたバケットの数。このメトリクスは、RIST、Zixi、SRT、または富士通 QoS プロトコルを使用するソースに適用されます。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN

メトリクス	説明
	• アベイラビリティーゾーン • すべてのフロー
SourceARQ Requests	自動再送要求 (ARQ) を通じて要求され、受信された再送信パケットの数。このメトリクスは、RIST、Zixi、SRT、または富士通 QoS プロトコルを使用するソースに適用されます。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceBitRate	受信 (ソース) ビデオのビットレート。 単位: ビット/秒 (b/s) 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー **Note** MediaConnect は、コンテンツ発信者のフローとサブスクライバーのフロー間のデータ接続を最適化するために、ヌルパケットを抑制します。その結果、サブスクライバーのフローのビットレートが変動したり、コンテンツ発信者のフローとサブスクライバーのフローのビットレートの間で違いが生じたりする可能性があります。ソースの健全性は、SourceBitRate と、SourceContinuityCounter や SourceNotRecoveredPackets などの他のメトリクスを組み合わせてモニタリングすることをお勧めします。

メトリクス	説明
SourceConnected	リソースのステータス。値 1 は、ソースが接続されたことを示します。値 0 (ゼロ) は、ソースが切断されたことを示します。このメトリクスは、Zixi、SRT、富士通、または RIST プロトコルを使用するソースにのみ適用されます。 単位: なし 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceDisconnections	ソースステータスが接続から切断に変わった回数。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceDroppedPackets	転送中に失われたパケット数。この値は、エラー修正が行われる前に測定されます。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceFEC Packets	前方誤り訂正 (FEC) を使用して送信され、受信されたパケットの数。このメトリクスは、RTP-FEC、Zixi、または富士通のプロトコルを使用する送信元にのみ適用されます。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceFEC Recovered	前方誤り訂正 (FEC) を使用して送信され、転送中に失われたパケットおよび回復されたパケットの数。このメトリクスは、RTP-FEC、Zixi、または富士通のプロトコルを使用する送信元にのみ適用されます。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceMergeActive	他のソースを基準にしたソースのステータスを示します。このメトリックは、フローにフェイルオーバーのソースが複数あり、Merge フェイルオーバーモードを使用している場合に役立ちます。値が 1 の場合は、フローに複数のソースがあり、このソースが 2022-7 のマージでアクティブに使用されていることを示します。0 (ゼロ) 値は、フローがソースを使用してストリームを形成していないことを示します。 単位: なし 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceSelected	ソースが、フローインジェストの入力として使用されているかどうかを示します。このメトリクスは、フローがソースフェイルオーバーを使用しており、フェイルオーバーモードがフェイルオーバーに設定されている場合に適用されます。値 1 は、ソースが入力として使用されていることを示します。0 (ゼロ) 値は、フローがバックアップストリームとして使用されていることを示します。 単位: なし 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceMergeLatency	このソースがプライマリソースを追跡する時間。このソースがプライマリソースの場合、値は 0 (ゼロ) です。 単位: ミリ秒 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceMergeStatusWarnMismatch	フローに不一致のソースが受信されていることを警告するステータスメトリクス。つまり、ドロップされたパケットは回復されず、ネットワークの信頼性が低下します。このメトリクスは、マージモードフェイルオーバーを使用するソースにのみ適用されます。マージモードのフェイルオーバーでは、両方のソースがバイナリで同一である必要があります。バイナリを同一にするには、ソースが同じエンコーダーからのものでなければなりません。これにより、パケットは同一であるので、ソース間で欠落しているパケットを共有できるようになります。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceMergeStatusWarnSolo	フローが受信するソースが 1 つだけであることを警告するステータスメトリクス。これは、ドロップされたパケットは回復されず、ネットワークの信頼性が低下することを意味します。このメトリクスは、マージモードフェイルオーバーを使用するソースにのみ適用されます。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceNotRecoveredPackets	転送中に失われ、エラー修正によって回復されなかったパケットの数。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceMissingPackets	両方のソースストリームからパケットが欠落していました。そのパケットは回復できなかったことを意味します。このメトリクスは、マージモードフェイルオーバーを使用するソースにのみ適用されます。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceOverflowPackets	ビデオが使用許容量よりも多くのバッファを必要としたために、転送中に失われたパケットの数。このメトリクスは、エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourcePacketLossPercent	回復したにも関わらず、転送中に失われたパケットの割合。 単位: パーセント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceRecoveredPackets	転送中に失われたが、回復したパケット数。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceRoundTripTime	ソースがシグナルを送信し、AWS Elemental MediaConnect からの確認を受信するまでにかかる時間。このメトリクスは、RIST、Zixi、SRT、または富士通 QoS プロトコルを使用するソースに適用されます。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位: ミリ秒 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceTotalPackets	受信されるパケットの総数。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceTotalBytes	ソースから MediaConnect に転送されたバイトの総量。 単位: バイト 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceDroppedPayloads	ソースから MediaConnect への転送中に失われたペイロード。ペイロードはビデオまたはオーディオサンプルのフレームです。ペイロードは、複数のパケットで構成できます。ペイロードメトリクスは CDI を使用する場合にのみ適用されます。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceLatePayloads	設定した最大同期バッファ時間枠外に到着したペイロードのパケット。ペイロードはビデオまたはオーディオサンプルのフレームです。ペイロードは、複数のパケットで構成できます。ペイロードメトリクスは CDI を使用する場合にのみ適用されます。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceTotalPayloads	ソースから MediaConnect に配信されたペイロードの総量。ペイロードはビデオまたはオーディオサンプルのフレームです。ペイロードは、複数のパケットで構成できます。ペイロードメトリクスは CDI を使用する場合にのみ適用されます。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

TR 101 290 プライオリティ 1 メトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信する TR 101 290 プライオリティ 1 のメトリクスが記載されています。

メトリクス	説明
SourceContinuityCounter	連続エラーが発生した回数。このエラーは、パケットの順序が正しくないか、パケットが失われたことを示しています。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourcePATError	プログラムアソシエーションテーブル (PAT) エラーが発生した回数。このエラーは PAT が欠落していることを示しています。PAT はトランスポートストリーム (TS) で利用可能なプログラムを一覧表示し、プログラムマップテーブル (PMT) を示します。デコーダーがその役割を果たすには PAT が必要です。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourcePIDError	パケット識別子 (PID) エラーが発生した回数。このエラーは、PID に関連するデータストリームが欠落していることを示します。PID は、ビデオ、オーディオ、およびデータストリームの場所を提供する識別子です。このエラーは、TS を多重化してから再度多重化した後に発生する可能性があります。 単位はカウント 有効なディメンション: • ソース ARN

メトリクス	説明
	• フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourcePMTError	プログラムマップテーブル (PMT) エラーが発生した回数。このエラーは、PMT が少なくとも 500 ミリ秒 (ms) ごとに受信されない場合に発生します。各 PMT には、デコーダーがデータを再構成するのに役立つ PID のリストが含まれています。デコーダーがその役割を果たすには PMT が必要です。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceTSByteError	TS バイトエラーが発生した回数。このエラーは、同期バイトが規定のバイト数を超えて表示されなかったことを示しています。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceTSSyncLoss	TS 同期喪失エラーが発生した回数。このエラーは、TS バイトエラーが 2 回以上連続した後に発生します。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

TR 101 290 プライオリティ 2 メトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信する TR 101 290 プライオリティ 2 のメトリクスが記載されています。

メトリクス	説明
SourceCATError	条件付きアクセステーブル (CAT) エラーが発生した回数。このエラーは、CAT が存在しないことを示しています。CAT は、統合レシーバーデコーダー (IRD) に、使用中の条件付きアクセス (CA) システムの管理メッセージの保存先を伝えます。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourceCRCError	巡回冗長検査 (CRC) エラーが発生した回数。このエラーは、CRC が、データが破損していると判断した場合に発生します。

メトリクス	説明
	単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourcePCRAccuracyError	プログラムクロックレジスター(PCR) の精度エラーが発生した回数。このエラーは、送信された PCR の値が予想値と 500 ナノ秒 (ns) 以上異なる場合に発生します。ストリームがエンコードされると、エンコーダーはエンコーダーのプログラムクロックから定期的に PCR 値を割り当てます。デコーダーはこれらの値に基づいてストリームの同期が保たれるようにします。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourcePCR Error	PCR エラーが発生した回数。このエラーは、PCR 値が十分な頻度で送信されない場合に発生します。このサービスは、ローカル 27 MHz のシステムクロックをリセットするために、一貫性のある頻繁な PCR に依存しています。このエラーは間隔が 100 ミリ秒 (ms) を超えると発生しますが、ベストプラクティスでは、PCR は少なくとも 40 ミリ秒ごとに受信するようになっています。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
SourcePTS Error	プレゼンテーションタイムスタンプ (PTS) エラーが発生した回数。このエラーは、少なくとも 700 ミリ秒ごとにプレゼンテーションタイムスタンプ (PTS) が受信されない場合に発生します。このエラーは、PTS の送信頻度が低いか、まったく送信されない場合に発生する可能性があります。このエラーの最も一般的な原因は、TS がスクランブルされる場合です。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
SourceTransportError	プライマリトランスポートエラーが発生した回数。このエラーは、TS パケットが使用できないことを示しています。このエラーが発生した場合は、このパケットのその他の TR 101 290 エラーをすべて無視してください。 単位はカウント 有効なディメンション: • ソース ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

出力の状態を監視するための AWS Elemental MediaConnect メトリクス

AWS Elemental MediaConnect は CloudWatch にメトリクスを送信します。特定のメトリクスを確認して、フローの出力の状態を評価できます。

> **Note**
>
> MediaConnect によって追跡されるメトリクスは、TR 101 290 仕様で定義されている基準に準拠しています。

メトリクス	説明
ConnectedOutputs	現在接続されている出力数。このメトリクスは、Zixi、Fujitsu、または SRT プロトコルを使用する出力にのみ適用されます。 単位はカウント 有効なディメンション: • フロー ARN • アベイラビリティーゾーン

メトリクス	説明
	• すべてのフロー
OutputConnected	出力のステータス。1 値は、出力が接続されたことを示します。0 (ゼロ) 値は、出力が切断されたことを示します。このメトリクスは、Zixi または SRT プロトコルを使用する出力にのみ適用されます。 単位: なし 有効なディメンション: • Outpost ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
OutputDisconnections	出力ステータスが接続から切断に変わった回数。 単位はカウント 有効なディメンション: • Outpost ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
OutputTotalBytes	MediaConnect から出力に転送されたバイトの総量。このメトリクスは CDI を使用する場合にのみ適用されます。 単位: バイト 有効なディメンション: • Outpost ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
OutputDroppedPayloads	MediaConnect から出力への転送中に失われたペイロード。ペイロードはビデオまたはオーディオサンプルのフレームです。ペイロードは、複数のパケットで構成できます。ペイロードメトリクスは CDI を使用する場合にのみ適用されます。 単位はカウント 有効なディメンション: • Outpost ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー
OutputLatePayloads	MediaConnect の内部バッファ外の出力に到達したペイロードのパケット。ペイロードはビデオまたはオーディオサンプルのフレームです。ペイロードは、複数のパケットで構成できます。ペイロードメトリクスは CDI を使用する場合にのみ適用されます。 単位はカウント 有効なディメンション: • Outpost ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
OutputTotalPayloads	MediaConnect から出力に配信されたペイロードの総量。ペイロードはビデオまたはオーディオサンプルのフレームです。ペイロードは、複数のパケットで構成できます。ペイロードメトリクスは CDI を使用する場合にのみ適用されます。 単位はカウント 有効なディメンション: • Outpost ARN • フロー ARN • アベイラビリティーゾーン • すべてのフロー

メディアの状態を監視するための AWS Elemental MediaConnect メトリクス

AWS Elemental MediaConnect は CloudWatch にメトリクスを送信します。特定のメトリクスを確認して、MediaConnect によって送信されたメディアの状態を評価できます。以下に示すメディアヘルスメトリクスは、トランスポートストリーム (TS) フローにのみ適用されます。各メトリクスの詳細については、このセクションの表を参照してください。

メディアメトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信するメトリクスクが記載されています。

メトリクス	説明
ConsecutiveDrops	MediaConnect との間でデータを送受信中に連続してドロップされたデータパケットの数。 単位はカウント サポートされるプロトコル:

メトリクス	説明
	• Zixi サポート対象の統計情報： • [Maximum] (最大) • Minimum • 平均 有効なディメンションセット: • フロー ARN • ソース ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
ConsecutiveNotRecovered	連続して復元されなかったデータパケットの数。データパケットがドロップされると、エラー修正によりそのパケットの復元が試みられます。このメトリクスは、長期間にわたってドロップされ復元されなかったデータパケットを特定するのに役立ちます。 単位はカウント サポートされるプロトコル: • Zixi サポート対象の統計情報： • [Maximum] (最大) • Minimum • 平均 有効なディメンションセット: • フロー ARN • ソース ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
Jitter	現在のネットワークジッター。ミリ秒単位で測定されます。ネットワークジッターは、レイテンシーの変化を測定したものです。ネットワークジッターが増加すると、レイテンシーにばらつきが生じていることを示し、品質に悪影響を及ぼす可能性があります。 単位: ミリ秒 (ms) サポートされるプロトコル: • すべてのトランスポートストリーム (TS) プロトコル サポート対象の統計情報： • [Maximum] (最大) • Minimum • 平均 有効なディメンションセット: • フロー ARN • ソース ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
Latency	フローまたはソースのストリームレイテンシー。レイテンシーは、データパケットがソースからMediaConnect に移動するのにかかる時間です。 単位: ミリ秒 (ms) サポートされるプロトコル: • すべてのトランスポートストリーム (TS) プロトコル サポート対象の統計情報： • [Maximum] (最大) • Minimum • 平均 有効なディメンションセット: • フロー ARN • ソース ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
ConnectionAttempts	接続試行の数。MediaConnect フローまたはソースが接続を失った場合、自動的に再接続を試行します。 単位はカウント サポートされるプロトコル: • Zixi • SRT リスナー • SRT コーラー サポート対象の統計情報： • Sum 有効なディメンションセット: • フロー ARN • ソース ARN • アベイラビリティーゾーン • すべてのフロー

メトリクス	説明
Uptime	ストリームがアクティブであった秒数。ストリームが切断されたり、接続タイムアウトになったりすると、このメトリクスはゼロにリセットされます。 単位はカウント サポートされるプロトコル: • すべてのトランスポートストリーム (TS) プロトコル サポート対象の統計情報 : • [Maximum] (最大) • Minimum • 平均 有効なディメンションセット: • フロー ARN • ソース ARN • アベイラビリティーゾーン • すべてのフロー

ゲートウェイの状態を監視するための AWS Elemental MediaConnect メトリクス

AWS Elemental MediaConnect は CloudWatch にメトリクスを送信します。特定のメトリクスを確認して、ゲートウェイの状態を評価できます。ゲートウェイに出入りするフローに問題がある場合、これらのメトリクスは問題の原因を突き止めるのに役立ちます。各メトリクスの詳細については、このセクションの表を参照してください。

> **Note**
>
> MediaConnect ゲートウェイのメトリクスは、高解像度時間 (1 秒) では利用できません。最低 1 分以上の時間を選択する必要があります。

トピック

ゲートウェイ入力のメトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信するゲートウェイ イングレスのメトリクスが記載されています。

メトリクス	説明
`IngressBridgeBitRate`	フェイルオーバーマージ後のイングレスブリッジのソースのビットレート。このソースは、ローカルデータセンターで生成されます。 単位: ビット/秒 (bps) 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
`IngressBridgeCATError`	条件付きアクセステーブル (CAT) エラーが発生した回数。このエラーは、CAT が存在しないことを示しています。CAT は、統合レシーバーデコーダー (IRD) に、使用中の条件付きアクセス (CA) システムの管理メッセージの保存先を伝えます。 単位はカウント 有効なディメンションセット:

メトリクス	説明
	• Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeCRCError	巡回冗長検査 (CRC) エラーが発生した回数。このエラーは、CRC が、データが破損していると判断した場合に発生します。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeContinuityCounter	連続エラーが発生した回数。このエラーは、パケットの順序が正しくないか、パケットが失われたことを示しています。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeDroppedPackets	転送中に失われたパケット数。この値は、エラー修正が行われる前に測定されます。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
IngressBridgeFailoverSwitches	ソースフェイルオーバーにフェイルオーバーモードを使用する場合に、ブリッジがソース間を行き来する合計回数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeMergeActive	ブリッジ上のすべてのソースのマージステータス。値 1 は、すべてのソースがマージされたことを示します。値 0 (ゼロ) は、少なくとも 1 つのソースが 2022-7 と能動的にマージされていないことを示します。 単位: なし 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeNotRecoveredPackets	転送中に失われ、エラー修正によって回復されなかったパケットの数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
IngressBridgePATError	プログラムアソシエーションテーブル (PAT) エラーが発生した回数。このエラーは PAT が欠落していることを示しています。PAT はトランスポートストリーム (TS) で利用可能なプログラムを一覧表示し、プログラムマップテーブル (PMT) を示します。デコーダーがその役割を果たすには PAT が必要です。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgePCRAccuracyError	プログラムクロックレジスター(PCR) の精度エラーが発生した回数。このエラーは、送信された PCR の値が予想値と 500 ナノ秒 (ns) 以上異なる場合に発生します。ストリームがエンコードされると、エンコーダーはエンコーダーのプログラムクロックに定期的に PCR 値を割り当てます。デコーダーはこれらの値に基づいてストリームの同期が保たれるようにします。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
IngressBridgePCRError	PCR エラーが発生した回数。このエラーは、PCR 値が十分な頻度で送信されない場合に発生します。このサービスは、ローカル 27 MHz のシステムクロックをリセットするために、一貫性のある頻繁な PCR に依存しています。このエラーは間隔が 100 ミリ秒 (ms) を超えると発生しますが、ベストプラクティスでは、PCR は少なくとも 40 ミリ秒ごとに受信するようになっています。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgePIDError	パケット識別子 (PID) エラーが発生した回数。このエラーは、PID に関連するデータストリームが欠落していることを示します。PID は、ビデオ、オーディオ、およびデータストリームの場所を提供する識別子です。このエラーは、トランスポートストリームを多重化してから再度多重化した後に発生する可能性があります。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
IngressBridgePMTError	プログラムマップテーブル (PMT) エラーが発生した回数。このエラーは、PMT が少なくとも 500 ミリ秒 (ms) ごとに受信されない場合に発生します。各 PMT には、デコーダーがデータを再構成するのに役立つ PID のリストが含まれています。デコーダーがその役割を果たすには PMT が必要です。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgePTSError	プレゼンテーションタイムスタンプ (PTS) エラーが発生した回数。このエラーは、少なくとも 700 ミリ秒ごとにプレゼンテーションタイムスタンプ (PTS) が受信されない場合に発生します。このエラーは、PTS の送信頻度が低いか、まったく送信されない場合に発生する可能性があります。このエラーの最も一般的な原因は、トランスポートストリーム (TS) がスクランブルされることです。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgePacketLossPercent	回復したにも関わらず、転送中に失われたパケットの割合。 単位: パーセント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
IngressBridgeRecoveredPackets	転送中に失われたが、回復したパケット数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeTSByteError	トランスポートストリームのバイトエラーが発生した回数。このエラーは、同期バイトが規定のバイト数を超えて表示されなかったことを示しています。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeTSSyncLoss	トランスポートストリームの同期損失エラーが発生した回数。このエラーは、トランスポートストリームのバイトエラーが 2 回以上連続した後に発生します。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
IngressBridgeTotalPackets	受信されるパケットの総数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
IngressBridgeTransportError	プライマリトランスポートエラーが発生した回数。このエラーは、トランスポートストリームパケットが使用できないことを示します。このエラーが発生した場合は、このパケットのその他の TR 101 290 エラーをすべて無視してください。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

ゲートウェイの入力ソースメトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信するゲートウェイイングレスソースのメトリクスが記載されています。

メトリクス	説明
IngressBridgeSourceARQRecovered	自動再送要求 (ARQ) によって回復された、ドロップされたバケットの数。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourceARQRequests	自動再送要求 (ARQ) を通じて要求され、受信された再送信パケットの数。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceBitRate	フェイルオーバーマージ前、、イングレスブリッジのソースのビットレート。このソースは、ローカルデータセンターで生成されます。 単位: ビット/秒 (bps) 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceCATError	条件付きアクセステーブル (CAT) エラーが発生した回数。このエラーは、CAT が存在しないことを示しています。CAT は、統合レシーバーデコーダー (IRD) に、使用中の条件付きアクセス (CA) システムの管理メッセージの保存先を伝えます。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourceCRCError	巡回冗長検査 (CRC) エラーが発生した回数。このエラーは、CRC が、データが破損していると判断した場合に発生します。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceContinuityCounter	連続エラーが発生した回数。このエラーは、パケットの順序が正しくないか、パケットが失われたことを示しています。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceDroppedPackets	転送中に失われたパケット数。この値は、エラー修正が行われる前に測定されます。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourceFECPackets	前方誤り訂正 (FEC) を使用して送信され、受信されたパケットの数。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceFECRecovered	前方誤り訂正 (FEC) を使用して送信され、転送中に失われたパケットおよび回復されたパケットの数。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceMergeActive	他のソースを基準にしたソースのステータスを示します。このメトリクスは、ブリッジにフェイルオーバーのソースが複数あり、Merge フェイルオーバーモードを使用している場合に役立ちます。値が 1 の場合、ブリッジには複数のソースがあり、このソースは 2022-7 のマージ時にアクティブに使用されていることを示します。0 (ゼロ) 値は、ブリッジがソースを使用してストリームを形成していないことを示します。 単位: なし 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourceMergeLatency	このソースがプライマリソースを追跡する時間。このソースがプライマリソースの場合、値は 0 (ゼロ) です。 単位: ミリ秒 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceNotRecoveredPackets	転送中に失われ、エラー修正によって回復されなかったパケットの数。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceOverflowPackets	ビデオが使用許容量よりも多くのバッファを必要としたために、転送中に失われたパケットの数。このメトリクスは、エンタイトルメントからコンテンツを受け取るフローや、複数のソースを持つフローには適用されません。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourcePATError	プログラムアソシエーションテーブル (PAT) エラーが発生した回数。このエラーは PAT が欠落していることを示しています。PAT はトランスポートストリーム (TS) で利用可能なプログラムを一覧表示し、プログラムマップテーブル (PMT) を示します。デコーダーがその役割を果たすには PAT が必要です。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourcePCRAccuracyError	プログラムクロックレジスター(PCR) の精度エラーが発生した回数。このエラーは、送信された PCR の値が予想値と 500 ナノ秒 (ns) 以上異なる場合に発生します。ストリームがエンコードされると、エンコーダーはエンコーダーのプログラムクロックから定期的に PCR 値を割り当てます。デコーダーはこれらの値に基づいてストリームの同期が保たれるようにします。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourcePCRError	PCR エラーが発生した回数。このエラーは、PCR 値が十分な頻度で送信されない場合に発生します。このサービスは、ローカル 27 MHz のシステムクロックをリセットするために、一貫性のある頻繁な PCR に依存しています。このエラーは間隔が 100 ミリ秒 (ms) を超えると発生しますが、ベストプラクティスでは、PCR は少なくとも 40 ミリ秒ごとに受信するようになっています。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourcePIDError	パケット識別子 (PID) エラーが発生した回数。このエラーは、PID に関連するデータストリームが欠落していることを示します。PID は、ビデオ、オーディオ、およびデータストリームの場所を提供する識別子です。このエラーは、トランスポートストリームを多重化してから再度多重化した後に発生する可能性があります。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourcePMTError	プログラムマップテーブル (PMT) エラーが発生した回数。このエラーは、PMT が少なくとも 500 ミリ秒 (ms) ごとに受信されない場合に発生します。各 PMT には、デコーダーがデータを再構成するのに役立つ PID のリストが含まれています。デコーダーがその役割を果たすには PMT が必要です。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourcePTSError	プレゼンテーションタイムスタンプ (PTS) エラーが発生した回数。このエラーは、少なくとも 700 ミリ秒ごとにプレゼンテーションタイムスタンプ (PTS) が受信されない場合に発生します。このエラーは、PTS の送信頻度が低いか、まったく送信されない場合に発生する可能性があります。このエラーの最も一般的な原因は、TS がスクランブルされる場合です。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourcePacketLossPercent	回復したにも関わらず、転送中に失われたパケットの割合。 単位: パーセント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourceRecoveredPackets	転送中に失われたが、回復したパケット数。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceRoundTripTime	ソースがシグナルを送信し、AWS Elemental MediaConnect からの確認を受信するまでにかかる時間。エンタイトルメントからコンテンツを受け取るフローには適用されません。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceTSByteError	トランスポートストリームのバイトエラーが発生した回数。このエラーは、同期バイトが規定のバイト数を超えて表示されなかったことを示しています。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

メトリクス	説明
IngressBridgeSourceTSSyncLoss	トランスポートストリームの同期損失エラーが発生した回数。このエラーは、トランスポートストリームのバイトエラーが 2 回以上連続した後に発生します。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceTotalPackets	受信されるパケットの総数。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名
IngressBridgeSourceTransportError	プライマリトランスポートエラーが発生した回数。このエラーは、トランスポートストリームパケットが使用できないことを示します。このエラーが発生した場合は、このパケットのその他の TR 101 290 エラーをすべて無視してください。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名 • ゲートウェイ ARN、インスタンス ID、ネットワーク名

ゲートウェイエぐレスメトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信するエングレスメトリクスが記載されています。

メトリクス	説明
EgressBridgeBitRate	フェイルオーバーマージ後のイーグレスブリッジのソースのビットレート。このソースは、MediaConnect フローで生成されます。 単位: ビット/秒 (bps) 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeCATError	条件付きアクセステーブル (CAT) エラーが発生した回数。このエラーは、CAT が存在しないことを示しています。CAT は、統合レシーバーデコーダー (IRD) に、使用中の条件付きアクセス (CA) システムの管理メッセージの保存先を伝えます。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeCRCError	巡回冗長検査 (CRC) エラーが発生した回数。このエラーは、CRC が、データが破損していると判断した場合に発生します。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeContinuityCounter	連続エラーが発生した回数。このエラーは、パケットの順序が正しくないか、パケットが失われたことを示しています。 単位はカウント 有効なディメンションセット:

メトリクス	説明
	• Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeDroppedPackets	転送中に失われたパケット数。この値は、エラー修正が行われる前に測定されます。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeFailoverSwitches	ソースフェイルオーバーにフェイルオーバーモードを使用する場合に、ブリッジがソース間を行き来する合計回数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeMergeActive	ブリッジ上のすべてのソースのマージステータス。値 1 は、すべてのソースがマージされたことを示します。値 0 (ゼロ) は、少なくとも 1 つのソースが 2022-7 と能動的にマージされていないことを示します。 単位: なし 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
EgressBridgeNotRecoveredPackets	転送中に失われ、エラー修正によって回復されなかったパケットの数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgePATError	プログラムアソシエーションテーブル (PAT) エラーが発生した回数。このエラーは PAT が欠落していることを示しています。PAT はトランスポートストリーム (TS) で利用可能なプログラムを一覧表示し、プログラムマップテーブル (PMT) を示します。デコーダーがその役割を果たすには PAT が必要です。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgePCRAccuracyError	プログラムクロックレジスター(PCR) の精度エラーが発生した回数。このエラーは、送信された PCR の値が予想値と 500 ナノ秒 (ns) 以上異なる場合に発生します。ストリームがエンコードされると、エンコーダーはエンコーダーのプログラムクロックに定期的に PCR 値を割り当てます。デコーダーはこれらの値に基づいてストリームの同期が保たれるようにします。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
EgressBridgePCRError	PCR エラーが発生した回数。このエラーは、PCR 値が十分な頻度で送信されない場合に発生します。このサービスは、ローカル 27 MHz のシステムクロックをリセットするために、一貫性のある頻繁な PCR に依存しています。このエラーは間隔が 100 ミリ秒 (ms) を超えると発生しますが、ベストプラクティスでは、PCR は少なくとも 40 ミリ秒ごとに受信するようになっています。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgePIDError	パケット識別子 (PID) エラーが発生した回数。このエラーは、PID に関連するデータストリームが欠落していることを示します。PID は、ビデオ、オーディオ、およびデータストリームの場所を提供する識別子です。このエラーは、トランスポートストリームを多重化してから再度多重化した後に発生する可能性があります。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
EgressBridgePMTError	プログラムマップテーブル (PMT) エラーが発生した回数。このエラーは、PMT が少なくとも 500 ミリ秒 (ms) ごとに受信されない場合に発生します。各 PMT には、デコーダーがデータを再構成するのに役立つ PID のリストが含まれています。デコーダーがその役割を果たすには PMT が必要です。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgePTSError	プレゼンテーションタイムスタンプ (PTS) エラーが発生した回数。このエラーは、少なくとも 700 ミリ秒ごとにプレゼンテーションタイムスタンプ (PTS) が受信されない場合に発生します。このエラーは、PTS の送信頻度が低いか、まったく送信されない場合に発生する可能性があります。このエラーの最も一般的な原因は、トランスポートストリーム (TS) がスクランブルされることです。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgePacketLossPercent	回復したにも関わらず、転送中に失われたパケットの割合。 単位: パーセント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
EgressBridgeRecoveredPackets	転送中に失われたが、回復したパケット数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeTSByteError	トランスポートストリームのバイトエラーが発生した回数。このエラーは、同期バイトが規定のバイト数を超えて表示されなかったことを示しています。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeTSSyncLoss	トランスポートストリームの同期損失エラーが発生した回数。このエラーは、トランスポートストリームのバイトエラーが 2 回以上連続した後に発生します。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

メトリクス	説明
EgressBridgeTotalPackets	受信されるパケットの総数。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID
EgressBridgeTransportError	プライマリトランスポートエラーが発生した回数。このエラーは、トランスポートストリームパケットが使用できないことを示します。このエラーが発生した場合は、このパケットのその他の TR 101 290 エラーをすべて無視してください。 単位はカウント 有効なディメンションセット: • Bridge ARN • ゲートウェイ ARN、インスタンス ID

ゲートウェイエぐレスソースメトリクス

次の表には、AWS Elemental MediaConnect が CloudWatch に送信するゲートウェイイングレスソースのメトリクスが記載されています。

メトリクス	説明
EgressBridgeSourceBitRate	フェイルオーバーマージ前の、イーグレスブリッジのソースのビットレート。このソースは、MediaConnect フローで生成されます。 単位: ビット/秒 (bps) 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクス	説明
EgressBridgeSourceCATError	条件付きアクセステーブル (CAT) エラーが発生した回数。このエラーは、CAT が存在しないことを示しています。CAT は、統合レシーバーデコーダー (IRD) に、使用中の条件付きアクセス (CA) システムの管理メッセージの保存先を伝えます。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourceCRCError	巡回冗長検査 (CRC) エラーが発生した回数。このエラーは、CRC が、データが破損していると判断した場合に発生します。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourceContinuityCounter	連続エラーが発生した回数。このエラーは、パケットの順序が正しくないか、パケットが失われたことを示しています。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクス	説明
EgressBridgeSourceDroppedPackets	転送中に失われたパケット数。この値は、エラー修正が行われる前に測定されます。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourceMergeActive	他のソースを基準にしたソースのステータスを示します。このメトリクスは、ブリッジにフェイルオーバーのソースが複数あり、Merge フェイルオーバーモードを使用している場合に役立ちます。値が 1 の場合、ブリッジには複数のソースがあり、このソースは 2022-7 のマージ時にアクティブに使用されていることを示します。0 (ゼロ) 値は、ブリッジがソースを使用してストリームを形成していないことを示します。 単位: なし 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourceMergeLatency	このソースがプライマリソースを追跡する時間。このソースがプライマリソースの場合、値は 0 (ゼロ) です。 単位: ミリ秒 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクス	説明
EgressBridgeSourceNotRecoveredPackets	転送中に失われ、エラー修正によって回復されなかったパケットの数。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourcePATError	プログラムアソシエーションテーブル (PAT) エラーが発生した回数。このエラーは PAT が欠落していることを示しています。PAT はトランスポートストリーム (TS) で利用可能なプログラムを一覧表示し、プログラムマップテーブル (PMT) を示します。デコーダーがその役割を果たすには PAT が必要です。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourcePCRAccuracyError	プログラムクロックレジスター(PCR) の精度エラーが発生した回数。このエラーは、送信された PCR の値が予想値と 500 ナノ秒 (ns) 以上異なる場合に発生します。ストリームがエンコードされると、エンコーダーはエンコーダーのプログラムクロックから定期的に PCR 値を割り当てます。デコーダーはこれらの値に基づいてストリームの同期が保たれるようにします。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクス	説明
EgressBridgeSourcePCRError	PCR エラーが発生した回数。このエラーは、PCR 値が十分な頻度で送信されない場合に発生します。このサービスは、ローカル 27 MHz のシステムクロックをリセットするために、一貫性のある頻繁な PCR に依存しています。このエラーは間隔が 100 ミリ秒 (ms) を超えると発生しますが、ベストプラクティスでは、PCR は少なくとも 40 ミリ秒ごとに受信するようになっています。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourcePIDError	パケット識別子 (PID) エラーが発生した回数。このエラーは、PID に関連するデータストリームが欠落していることを示します。PID は、ビデオ、オーディオ、およびデータストリームの場所を提供する識別子です。このエラーは、トランスポートストリームを多重化してから再度多重化した後に発生する可能性があります。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクス	説明
EgressBridgeSourcePMTError	プログラムマップテーブル (PMT) エラーが発生した回数。このエラーは、PMT が少なくとも 500 ミリ秒 (ms) ごとに受信されない場合に発生します。各 PMT には、デコーダーがデータを再構成するのに役立つ PID のリストが含まれています。デコーダーがその役割を果たすには PMT が必要です。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourcePTSError	プレゼンテーションタイムスタンプ (PTS) エラーが発生した回数。このエラーは、少なくとも 700 ミリ秒ごとにプレゼンテーションタイムスタンプ (PTS) が受信されない場合に発生します。このエラーは、PTS の送信頻度が低いか、まったく送信されない場合に発生する可能性があります。このエラーの最も一般的な原因は、TS がスクランブルされる場合です。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourcePacketLossPercent	回復したにも関わらず、転送中に失われたパケットの割合。 単位: パーセント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクス	説明
EgressBridgeSourceRecoveredPackets	転送中に失われたが、回復したパケット数。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourceTSByteError	トランスポートストリームのバイトエラーが発生した回数。このエラーは、同期バイトが規定のバイト数を超えて表示されなかったことを示しています。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourceTSSyncLoss	トランスポートストリームの同期損失エラーが発生した回数。このエラーは、トランスポートストリームのバイトエラーが 2 回以上連続した後に発生します。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクス	説明
EgressBridgeSourceTotalPackets	受信されるパケットの総数。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン
EgressBridgeSourceTransportError	プライマリトランスポートエラーが発生した回数。このエラーは、トランスポートストリームパケットが使用できないことを示します。このエラーが発生した場合は、このパケットのその他の TR 101 290 エラーをすべて無視してください。 単位はカウント 有効なディメンションセット: • ブリッジ ARN、ブリッジソース名、フロー ARN • ゲートウェイ ARN、インスタンス ID、アベイラビリティーゾーン

メトリクスによるトラブルシューティング

AWS Elemental MediaConnect が CloudWatch に送信するメトリクスを確認することで、ストリームの状態をモニタリングできます。特に、MediaConnect フローで問題が発生した場合、これらのメトリクスは問題の切り分けに役立ちます。監視すべき具体的なメトリクスは、ソースが使用するプロトコルによって異なります。ソースプロトコル別にソートされた以下のリストを確認してください。

トピック

- ソースが RIST プロトコルを使用しているかどうかを監視するメトリクス
- ソースが RTP プロトコルを使用しているかどうかを監視するメトリクス
- ソースが RTP-FEC プロトコルを使用しているかどうかを監視するメトリクス
- ソースが SRT プロトコルを使用しているかどうかを監視するメトリクス
- ソースが Zixi プッシュプロトコルを使用しているかどうかを監視するメトリクス
- ソースがエンタイトルメントからのものかどうかを監視するメトリクス

- ゲートウェイを使用している場合に監視するメトリクス

ソースが RIST プロトコルを使用しているかどうかを監視するメトリクス

ソースのプロトコルが RIST の場合は、以下のメトリクスを見てソースの状態を評価してください。

- ARQRecovered
- ARQRequests
- DroppedPackets
- NotRecoveredPackets
- OverflowPackets
- PacketLossPercent
- RecoveredPackets
- RoundTripTime
- TotalPackets

ソースが RTP プロトコルを使用しているかどうかを監視するメトリクス

ソースのプロトコルが RTP の場合は、以下のメトリクスを見てソースの状態を評価してください。

- DroppedPackets
- OverflowPackets
- RoundTripTime
- TotalPackets

ソースが RTP-FEC プロトコルを使用しているかどうかを監視するメトリクス

ソースのプロトコルが RTP-FEC の場合は、以下のメトリクスを見てソースの状態を評価してください。

- DroppedPackets
- FECPackets
- FECRecovered
- NotRecoveredPackets

- OverflowPackets
- RecoveredPackets
- RoundTripTime
- TotalPackets

ソースが SRT プロトコルを使用しているかどうかを監視するメトリクス

ソースのプロトコルが SRT (リスナーまたはコーラー) の場合は、以下のメトリクスを見てソースの状態を評価してください。

- ARQRecovered
- ARQRequests
- DroppedPackets
- NotRecoveredPackets
- OverflowPackets
- RecoveredPackets
- RoundTripTime
- TotalPackets

ソースが Zixi プッシュプロトコルを使用しているかどうかを監視するメトリクス

ソースのプロトコルが Zixi プッシュの場合は、以下のメトリクスを見てソースの状態を評価してください。

- ARQRecovered
- ARQRequests
- DroppedPackets
- FECPackets
- FECRecovered
- NotRecoveredPackets
- OverflowPackets
- RecoveredPackets

- RoundTripTime
- TotalPackets

ソースがエンタイトルメントからのものかどうかを監視するメトリクス

ソースが、別のAWSアカウントから自分のアカウントに付与されたエンタイトルメントからのものである場合は、以下のメトリクスを確認してソースの状態を評価してください。

- ARQRecovered
- ARQRequests
- DroppedPackets
- FECPackets
- FECRecovered
- NotRecoveredPackets
- OverflowPackets
- RecoveredPackets
- RoundTripTime
- TotalPackets

ゲートウェイを使用している場合に監視するメトリクス

以下のメトリクスを見て、ゲートウェイの状態を評価してください。

Ingress Bridge を伴うゲートウェイを使用している場合に監視するメトリクス

以下のメトリクスを見て、ゲートウェイのイングレスブリッジの状態を評価してください。Ingress Bridge のトラブルシューティングに関する推奨メトリクスはプロトコルごとに分けられています。

- RTP
  - IngressBridgeTotalPackets
  - IngressBridgeDroppedPackets
  - IngressBridgeSourceTotalPackets
  - IngressBridgeSourceDroppedPackets
  - IngressBridgeSourceOverflowPackets

  - IngressBridgeSourceRoundTripTime

- RTP-FEC
  - IngressBridgeTotalPackets
  - IngressBridgeDroppedPackets
  - IngressBridgeRecoveredPackets
  - IngressBridgeNotRecoveredPackets
  - IngressBridgeSourceTotalPackets
  - IngressBridgeSourceDroppedPackets
  - IngressBridgeSourceRecoveredPackets
  - IngressBridgeSourceNotRecoveredPackets
  - IngressBridgeSourceOverflowPackets
  - IngressBridgeSourceFECPackets
  - IngressBridgeSourceFECRecovered
  - IngressBridgeSourceRoundTripTime
- UDP
  - IngressBridgeTotalPackets
  - IngressBridgeSourceTotalPackets
  - IngressBridgeSourceOverflowPackets

イーグレスブリッジを伴うゲートウェイを使用している場合に監視するメトリクス

以下のメトリクスを見て、ゲートウェイのイーグレスブリッジの状態を評価してください。

- EgressBridgeTotalPackets
- EgressBridgeDroppedPackets
- EgressBridgeRecoveredPackets
- EgressBridgeNotRecoveredPackets
- EgressBridgeSourceTotalPackets
- EgressBridgeSourceDroppedPackets
- EgressBridgeSourceRecoveredPackets
- EgressBridgeSourceNotRecoveredPackets

CloudWatch Events を使用したモニタリング

Amazon CloudWatch Events を使用すると、AWS のサービスを自動化し、アプリケーションの可用性の問題やリソースの変更などのシステムイベントに自動的に応答することができます。AWS のサービスからのイベントは、ほぼリアルタイムに CloudWatch Events に送信されます。簡単なルールを記述して、注目するイベントと、イベントがルールに一致した場合に自動的に実行するアクションを指定できます。

自動的にトリガーできるオペレーションには、以下が含まれます:

- AWS Lambda 関数の呼び出し
- Amazon EC2 Run Command の呼び出し
- Amazon Kinesis Data Streams へのイベントの中継
- AWS Step Functions ステートマシンのアクティブ化
- Amazon SNS トピックまたは Amazon SQS キューの通知

詳細については、「Amazon CloudWatch Events ユーザーガイド」を参照してください。

MediaConnect の CloudWatch Events

- AWS Elemental MediaConnect フロー状態の変更イベント
- AWS Elemental MediaConnect フローのメンテナンスイベント
- AWS Elemental MediaConnect のヘルスイベントフロー
- AWS Elemental MediaConnect アラートイベント
- AWS Elemental MediaConnect ソースのヘルスイベント
- AWS Elemental MediaConnect で出力を検証するには

AWS Elemental MediaConnect フロー状態の変更イベント

このイベントは、フローの状態が [スタンバイ]、[アクティブ]、[更新中]、[削除]、[開始]、[停止]、または [エラー] のいずれかの状態から変化したときに公開されます。

このイベントにサブスクライブする方法については、Amazon CloudWatch を参照してください。

以下のメッセージは、このCloudWatchのイベントの例です。

```
{
```

```
    "account": "111122223333",
    "detail": {
        "currentStatus": "STARTING",
        "previousStatus": "STANDBY"
    },
    "detail-type": "MediaConnect Flow Status Change",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "region": "us-east-1",
    "resources": ["arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:AwardsShow"],
    "source": "aws.mediaconnect",
    "time": "2022-01-06T00:45:47Z",
    "version": "0"
}
```

AWS Elemental MediaConnect フローのメンテナンスイベント

このイベントは、フローのメンテナンスステータスが以下のいずれかの状態に、または次の状態から変化したときに公開されます:

- スケジュール済み-フローのメンテナンスが予定されています。
- 再スケジュール-MediaConnect は、以前に予定されていた日時にメンテナンスを実行することができません。このフローのメンテナンスのために、MediaConnect によって新しい日付と時刻が自動的に割り当てられました。
- キャンセル-このフローのメンテナンスは MediaConnect によってキャンセルされました。
- 進行中-このフローのメンテナンスが開始され、現在進行中です。
- 終了-このフローのメンテナンスは正常に完了しました。
- 失敗-このフローのメンテナンスは正常に完了しませんでした。

このイベントにサブスクライブする方法については、Amazon CloudWatch を参照してください。

MediaConnect のメンテナンスについて詳しくは、「MediaConnect フローのメンテナンス」を参照してください。

以下のメッセージは、このCloudWatchのイベントの例です。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
```

```
    "detail-type": "MediaConnect Flow Maintenance",
    "source": "aws.mediaconnect",
    "account": "111122223333",
    "time": "2022-02-14T00:45:47Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1:23aBC45dEF67hiJ8:12AbC34DE5fG:ExampleFlow"
    ],
    "detail": {
        "currentStatus": "FINISHED"
    }
}
```

AWS Elemental MediaConnect のヘルスイベントフロー

AWS Elemental MediaConnect は、ヘルスインジケーターフローの状態が変化した後にヘルスイベントフローを公開します。

MediaConnect は、次の 1 つ以上のヘルスインジケーターフローの状態が変化した場合はいつでもこのイベントを公開します。このイベントは、フローの現在の状態と以前の状態を公開します。

フローの健全性は次のとおりです:

- ソースステート
  - 考えられる状態:`connected`、`receiving`、`disconnected`、`idle`
- フェイルオーバー· スイッチ
  - 考えられる状態:`true`、`false`
- TR-101: TR-101は、トランスポートストリーム (TS) のモニタリングに関する業界標準の技術的推奨事項です。以下のイベントは TS ベースのプロトコルについてのみ公開されています。
  - TS 同期損失とは、`true`が、ソースペイロードが有効なトランスポートストリームには見えない場合に起きます。
  - 連続カウントエラーとは、`true`がソース側で連続カウントエラーが見つかった場合に起きます。
  - トランスポートエラーとは、`true`が、TS にトランスポートインジケーターが設定されている場合に起きます。
  - PCR エラーとは、`true`がPCR パケットの受信に PCR の連続性がなかったり、ギャップが長かったりする場合に起きます。

このイベントにサブスクライブする方法については、Amazon CloudWatch を参照してください。

以下のメッセージは、このCloudWatchのイベントの例です。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "MediaConnect Flow Health",
  "source": "aws.mediaconnect",
  "account": "012345678901",
  "time": "2006-01-02T15:04:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediaconnect:us-
east-1:012345678901:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow"
  ],
  "detail": {
    "unhealthy": true,
    "current": {
      "failover_switch": false,
      "source_state": "CONNECTED",
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": true,
        "transport_error": true,
        "pcr_error": true
      }
    },
    "previous": {
      "failover_switch": false,
      "source_state": "CONNECTED",
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": false,
        "transport_error": false,
        "pcr_error": false
      }
    }
  }
}
```

AWS Elemental MediaConnect アラートイベント

リソースでエラーが発生すると、MediaConnect はアラートイベントを公開します。イベントには、エラーコードと問題を説明するメッセージが含まれます。これらのアラートは、MediaConnect コンソールに表示されるか、`describe-flow` AWS Command Line Interface (AWS CLI) コマンドを使用して表示されます。`describe-flow` コマンドの詳細については、「AWS CLI コマンドリファレンス」を参照してください。

このイベントにサブスクライブする方法については、Amazon CloudWatch を参照してください。

以下のメッセージは、このCloudWatchのイベントの例です。

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-0123456789ab",
 "detail-type": "MediaConnect Alert",
 "source": "aws.mediaconnect",
 "account": "111122223333",
 "time": "2022-01-06T00:45:47Z",
 "region": "us-east-1",
 "resources": [
 "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow"
 ],
 "detail": {
 "errored": true,
 "error-code": "AccessDeniedException",
 "error-message": "Permission denied accessing encryption key for output
 Test. Removing output until it is fixed (secret arn:aws:secretsmanager:us-
east-1:111122223333:secret:ExampleSecret, role arn:aws:iam::111122223333:role/
ExampleKey)"
 }
}
```

AWS Elemental MediaConnect ソースのヘルスイベント

AWS Elemental MediaConnectは、ソースのヘルスインジケーターの状態が変化した後に、ソースのヘルスイベントを公開します。

MediaConnect は、次の 1 つ以上のソースのヘルスインジケーターの状態が変化した場合はいつでもこのイベントを公開します。このイベントは、フローの現在の状態と以前の状態を公開します。ソー

スのヘルスイベントでは、影響を受けるフローとソースがresourcesセクションに一覧表示されていることに注意してください。

ソースのヘルスメトリクスは次のとおりです:

- ソースステート
  - 考えられる状態:connected、receiving、disconnected、idle
- TR-101: TR-101は、トランスポートストリーム (TS) のモニタリングに関する業界標準の技術的推奨事項です。以下のイベントは TS ベースのプロトコルについてのみ公開されています。
  - TS 同期損失-ソースペイロードが有効なトランスポートストリームには見えない場合は、当てはまります。
  - 連続カウントエラー -ソースが連続カウントエラーを検出した場合は、当てはまります。
  - トランスポートエラー-TS にトランスポートインジケーターが設定されている場合は、当てはまります。
  - PCR エラー-PCR パケットの受信に PCR が連続していない場合や、ギャップが長い場合は、当てはまります。。

このイベントにサブスクライブする方法については、Amazon CloudWatch を参照してください。

以下のメッセージは、このCloudWatchのイベントの例です。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "MediaConnect Source Health",
  "source": "aws.mediaconnect",
  "account": "012345678901",
  "time": "2006-01-02T15:04:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediaconnect:us-
east-1:012345678901:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow",
    "arn:aws:mediaconnect:us-
east-1:012345678901:source:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleSource"
  ],
  "detail": {
    "unhealthy": true,
    "current": {
      "source_state": "CONNECTED",
```

```
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": true,
        "transport_error": true,
        "pcr_error": true
      }
    },
    "previous": {
      "source_state": "CONNECTED",
      "tr101": {
        "ts_sync_loss": false,
        "continuity_count_error": false,
        "transport_error": false,
        "pcr_error": false
      }
    }
  }
}
```

AWS Elemental MediaConnect で出力を検証するには

AWS Elemental MediaConnect出力ヘルスインジケーターの状態が変化した後に、出力ヘルスイベントを公開します。

MediaConnect は、次の 1 つ以上の出力ヘルスインジケーターの状態に変化があるたびに、このイベントを公開します。このイベントは、フローの現在の状態と以前の状態を公開します。出力ヘルスイベントでは、影響を受けるフローと出力がresourcesセクションに一覧表示されていることに注意してください。

出力ヘルスインジケーターは次のとおりです:

- 出力状態
  - 考えられる状態:connected、receiving、disconnected、idle

このイベントにサブスクライブする方法については、Amazon CloudWatch を参照してください。

以下のメッセージは、このCloudWatchのイベントの例です。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "MediaConnect Output Health",
```

```
  "source": "aws.mediaconnect",
  "account": "012345678901",
  "time": "2006-01-02T15:04:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:mediaconnect:us-
east-1:012345678901:flow:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleFlow",
    "arn:aws:mediaconnect:us-
east-1:012345678901:output:1:AbCdEfGhIjKlMnOp:abcdef123455:ExampleOutput"
  ],
  "detail": {
    "current": {
      "output_state": "CONNECTED"
    },
    "previous": {
      "output_state": "DISCONNECTED"
    }
  }
}
```

AWS CloudTrail を使用した AWS Elemental MediaConnect API コールのログ記録

AWS Elemental MediaConnect は AWS CloudTrail (ユーザー、ロール、または AWS Elemental MediaConnect の AWS のサービスによって実行されるアクションを記録するサービス) と統合されています CloudTrail のすべての API コールをイベントとして AWS Elemental MediaConnect にキャプチャします。キャプチャされたコールには、AWS Elemental MediaConnect コンソールからの呼び出しと AWS Elemental MediaConnect API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、AWS Elemental MediaConnect のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail で収集された情報を使用して、AWS Elemental MediaConnect に対するリクエスト、リクエスト元の IP アドレス、リクエストの実行者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrail での AWS Elemental MediaConnect についての情報

AWS アカウントを作成すると、そのアカウントに対して CloudTrail が有効になります。AWS Elemental MediaConnect でアクティビティが発生すると、そのアクティビティは [イベント履歴] に

ある他の AWS のサービスイベントとともに、CloudTrail イベントに記録されます。AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

AWS Elemental MediaConnect のイベントを含めた AWS アカウント内のイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべての AWS リージョンに適用されます。追跡は、AWSパーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集したイベントデータをより詳細に分析し、それに基づく対応するためにその他の AWS のサービスを設定できます。詳細については、次を参照してください。

- 証跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail の通知の設定
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

すべての AWS Elemental MediaConnect アクションは CloudTrail によってログに記録され、AWS Elemental MediaConnect API リファレンス に記載されています。例えば、`CreateFlow`、`StartFlow`、および `UpdateFlowOutput` オペレーションへの呼び出しによって CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「[CloudTrail userIdentity 要素」を参照してください。

AWS Elemental MediaConnect でのログファイルエントリについて

証跡は、指定した Simple Storage Service (Amazon S3) バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、単一または複数のログエントリがあります。各イベントは任意の送信元からの単一のリクエストを表し、リクエストされたオペレーション、オペレーションの日時、リクエストパラメーターなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

`DescribeFlow` オペレーションを示す CloudTrail ログエントリの例は、次のとおりです。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "ABCDEFGHIJKL123456789",
    "arn": "arn:aws:sts::111122223333:user/testUser",
    "accountId": "111122223333",
    "accessKeyId": "ABCDE12345EFGHIJKLMN",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-16T20:34:51Z",
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ABCDEFGHIJKL123456789",
        "arn": "arn:aws:iam::111122223333:role/Administrator",
        "accountId": "111122223333",
        "userName": "Administrator",
      },
    },
  },
  "eventTime": "2018-11-16T20:34:52Z",
  "eventSource": "mediaconnect.amazonaws.com",
  "eventName": "DescribeFlow",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.17",
  "userAgent": "aws-cli/1.15.40 Python/3.6.5 Darwin/16.7.0 botocore/1.10.40",
  "requestParameters": {
    "flowArn": "arn%3Aaws%3Amediaconnect%3Aus-west-2%111122223333%3Aflow
%3A1-23aBC45dEF67hiJ8-12AbC34DE5fG%3AAwardsShow",
```

```
  },
  "responseElements": {
  },
  "requestID": "1a2b3c4d-1234-5678-1234-1a2b3c4d5e6f",
  "eventID": "987abc65-1a2b-3c4d-5d6e-987abc654def",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333",
}
```


フローとソースの状態を監視する

AWS Elemental MediaConnectコンソールでは、フローとそのソースの状態をモニタリングできます。

フローの状態は、エンタイトルメントまたは暗号化の問題によりフローが接続されていないかどうかを示します。

ソース状態には、ソースが接続されているかどうかが示されます。その場合、コンソールには一定期間のソースのステータスを示す Amazon CloudWatch メトリクスが表示されます。

トピック

- フローの状態をモニタリングする
- ソースの状態を監視する

フローの状態をモニタリングする

MediaConnect コンソールの [アラート] タブには、現在のフローを開始または停止したときに発生したアラートのリストが表示されます。フローのアラートの全リストについては、「Amazon CloudWatch」を参照してください。

MediaConnect は [アラート] タブに次のアラートを表示します:

- ストリームエラーと呼ばれる、フローに関するコンテキストエラーメッセージ。
- このフローの基になっているエンタイトルメントはすでに使用されています。これは、同じエンタイトルメントに基づいて複数のフローを作成した場合に発生します。これらのフローのいずれかがすでに実行されている場合、2 つ目のフローを開始しようとすると、MediaConnect はアラートを表示します。

- このフローの基になっているエンタイトルメントはもう存在しません。これは、エンタイトルメントを付与したアカウント (コンテンツ作成者) がエンタイトルメントを取り消した場合に発生します。
- このフローの基になっているエンタイトルメントにはアクティブなソースがありません。これは、送信元のフローが削除または停止された場合に発生します。そのエンタイトルメントに基づいてフローを開始すると、作成者のフローからのコンテンツはありません。
- フローの復号化または暗号化情報が無効です。これには、いくつかの理由が考えられます。例えば、復号化キーが指定されたアルゴリズムのタイプと一致しない場合などです。または、フローが SPEKE 暗号化を使用するエンタイトルメントに基づいていて、MediaConnect が条件付きアクセス (CA) プラットフォームキープロバイダーにアクセスできない場合もあります。
- フローはエンタイトルメントに基づいており、コンテンツ作成者のフローにはすでに最大数の出力があります。

ストリームエラー

MediaConnect アラートには、フローのソースと出力に関するコンテキストエラーが含まれる場合もあります。これらはストリームエラーと呼ばれ、特定のフォーマットに従います。

- ソース *####*ストリームエラー：*########*。フローのソースを調べてください。
- 出力 *###*ストリームエラー：*########*。フロー出力を調べてください。

エラーメッセージには問題の詳しい内容が示され、トラブルシューティングをどこから始めればよいかを示す指標として使用できます。

例

NationalBroadcastという名前のフローで、次のアラートを受け取った場合:

ソース *StudioFeed2* ストリームエラー：*CDI #####*。フローのソースを調べてください。

これは、ソースのインバウンド CDI にエラーがあることを示しています。具体的には、次のステップは NationalBroadcastという名前のフロー上の StudioFeed2ソースの設定を確認することです。インバウンドポート、使用されているVPC インターフェイス、メディアストリームなどの CDI 固有のソース設定には、特に注意する必要があります。

フローアラートを表示する

アクティブなアラート(コンソール)をすべて表示するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediapackage/) を開きます。
2. [フロー] ページで、フローの名前を選択します。
3. [エージェント] タブを選択します。

   このサービスは、フロー上のアラート (ある場合) のリストを表示します。

ソースの状態を監視する

AWS Elemental MediaConnectのコンソールでは、一定期間のソースの状態を示す Amazon CloudWatch メトリクスを表示できます。ソースの状態は次のメトリクスで報告されます:

- ソースビットレート — 受信動画のビットレート。
- 受信パケットの総数 — MediaConnect が受信したパケットの総数。

ソース (コンソール) の状態を監視するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediapackage/) を開きます。
2. [フロー] ページで、フローの名前を選択します。
3. 「ソース」タブを選択し、ソースのステータスを表示します。これには、以下のものが含まれます :

   - 「ソースの状態」フィールドには、ソースの現在の状態が表示されます。
     - [接続] は、フローがソースに正常に接続されたことを示します。
     - [接続切断] は、フローがソースに接続されていないことを示します。この問題を解決するには、ソースが実際にコンテンツを送信していることを確認します。また、許可リスト CIDR やプロトコル設定など、フローのソース設定も確認します。
     - フローが非アクティブであることは、フローがまだ開始されていないことを示しています。この問題を解決するには、フローを開始します。
     - エラーは、MediaConnect に CloudWatch と通信する許可がないことを示します。このエラーを解決するには、MediaConnect が CloudWatch からメトリクス統計を取得できるようにするエンティティとして、AWS マネジメントコンソールにサインインする必要があります。ガイダンスとして、こちらの例を参照してください。

- ソースの状態のメトリクスセクションは、ソースの状態が [接続] の場合にのみ表示されます。グラフには、ソースビットレートと過去 1 時間に受信した合計パケット数が表示されます。セクションの右上にあるドロップダウンから別の期間を選択できます。

> **Note**
>
> MediaConnect は、選択した期間に応じて、1 分、5 分、または 30 分ごとに自動的に CloudWatch からのデータを更新します。チャートが更新される場合、データはリアルタイムより 1 分遅れます。

AWS Elemental MediaConnect リソースのタグ付け

タグとは、お客様または AWS が AWS リソースに割り当てるカスタム属性ラベルです。各タグは 2 つの部分で構成されます。

- タグキー (例： `CostCenter`、`Environment`、または `Project`)。タグキーでは、大文字と小文字が区別されます。
- タグ値として知られるオプションのフィールド (例： `111122223333` または `Production`)。タグ値を省略すると、空の文字列を使用した場合と同じになります。タグキーと同様に、タグ値は大文字と小文字が区別されます。

タグは、以下のことに役立ちます。

- AWS リソースの特定と整理。多くの AWS サービスではタグ付けがサポートされるため、さまざまなサービスからリソースに同じタグを割り当てて、リソースの関連を示すことができます。たとえば、AWS Elemental MediaLiveチャンネル出力に割り当てるのと同じタグを AWS Elemental MediaConnect フローに割り当てることができます。
- AWS のコストの追跡。これらのタグは、AWS Billing and Cost Management ダッシュボードで有効にします。AWS では、タグを使用してコストを分類し、毎月のコスト配分レポートを提供します。詳細については、「AWS Billing ユーザーガイド」の「Use Cost Allocation Tags」(コスト配分タグの使用) を参照してください。

以下のセクションでは、AWS Elemental MediaConnect のタグに関する詳細を示します。

トピック

AWS Elemental MediaConnect でサポートされているリソース

AWS Elemental MediaConnect の以下のリソースがタグ付けをサポートしています。

- フロー
- [Sources] (出典)
- [Outputs] (出力)
- 使用権限管理

タグの追加と管理の詳細については、「タグの管理」を参照してください。

AWS Elemental MediaConnect は AWS Identity and Access Management (IAM) のタグベースのアクセスコントロール機能をサポートしていません。

タグの命名規則と使用規則

AWS Elemental MediaConnect リソースでのタグの使用には、次の基本的な命名規則と使用規則が適用されます。

- 各リソースには、最大 50 個のタグを設定できます。
- タグキーは、リソースごとにそれぞれ一意である必要があります。また、各タグキーに設定できる値は 1 つのみです。
- タグキーの最大長は UTF-8 で 128 Unicode 文字です。
- タグ値の最大長は UTF-8 で 256 Unicode 文字です。
- 使用できる文字は、UTF-8 対応の文字、数字、スペースと、文字 (. : + = @ _ / -) (ハイフン) です。Amazon EC2 リソースでは、任意の文字を使用できます。
- タグのキーと値は大文字と小文字が区別されます。ベストプラクティスとして、タグを大文字にするための戦略を決定し、その戦略をすべてのリソースタイプにわたって一貫して実装します。たとえば、`Costcenter`、`costcenter`、`CostCenter` のいずれを使用するかを決定し、すべてのタグに同じ規則を使用します。大文字と小文字の扱いについて、同様のタグに整合性のない規則を使用することは避けてください。

- プレフィックス `aws:` はタグで使用することはできません。AWS 用に予約されています。このプレフィックスが含まれるタグのキーや値を編集または削除することはできません。このプレフィックスの付いたタグは、リソースあたりのタグ数のクォータにカウントされません。

タグの管理

タグは、リソースの `Key` および `Value` プロパティで構成されています。このようなプロパティの値を追加、編集、削除するには、AWS Elemental MediaConnect コンソール、AWS CLI、または AWS Elemental MediaConnect API を使用できます。タグの使用については、以下を参照してください。

- AWS Elemental MediaConnect API リファレンスのリソース
- このガイドの「the section called “フロー上のタグの管理”」
- このガイドの「the section called “ソースのタグの管理”」
- このガイドの「the section called “出力のタグの管理”」
- このガイドの「the section called “エンタイトルメントのタグ管理”」

MediaConnect フローメンテナンス

セキュリティ、信頼性、運用パフォーマンスを確保するため、AWS Elemental MediaConnect は基盤となるシステムのメンテナンスを定期的に実行します。メンテナンスアクティビティには、オペレーティングシステムのパッチ適用、ドライバーの更新、ソフトウェアとパッチのインストールなどのアクションが含まれます。

> **Note**
>
> メンテナンスプロセスの一環として、フローを再起動する必要があります。

メンテナンスイベントが発生する日と時刻を選択できます。これは、メンテナンスウィンドウと呼ばれ、メンテナンスイベントが必要になるたびに使用されます。曜日と時刻を変更する必要がある場合は、メンテナンスウィンドウを編集できます。

フローのメンテナンスが必要な場合、AWS がフローに 必要期限 日を割り当てます。フローにメンテナンスウィンドウが設定されていない場合は、「メンテナンスウィンドウの設定」を参照してください。メンテナンスが必要なフローは、MediaConnect コンソールで確認できます。または AWS CLI を使用して、「メンテナンスが必要なフローの表示」を参照してください。フローに 必要期限 日が割り当てられている場合は、メンテナンスを実施する特定の日付を選択できます。選択した メンテナンス日 は、次のメンテナンスイベントにのみ適用されます。

メンテナンスウィンドウを設定しない場合は、AWS が自動的にメンテナンスウィンドウを選択します。フローごとにメンテナンスウィンドウを設定し、MediaConnect がそのウィンドウ内に自動的に再起動を実行できるようにすることをお勧めします。MediaConnect に再起動を許可すると、フローのダウンタイムが短くなります。フローにメンテナンスが必要で、手動でフローを再起動することを選択した場合、そのフローのメンテナンスの状態は キャンセル済み に変わります。手動で再起動したフローには必要な更新が引き続き適用されますが、正常に完了しました ステータスは表示されません。再起動を手動で実行したため、MediaConnect はそのフローの更新を行う必要がなくなり、メンテナンスは キャンセル済み と見なされます。

メンテナンスウィンドウの期間は 2 時間です。

> **Important**
>
> 期間が 2 時間であっても、フローへの影響が 2 時間続くわけではありません。2 時間以内のある時点で、フローは通常の停止と開始を行います。

例: フローのメンテナンスウィンドウの 開始時間 を 02:00 に設定すると、フローは 02:00 から 04:00 の間のある時点に再起動されます。

スケジュールされた日時にメンテナンスが行われない場合、MediaConnect は翌週のメンテナンスウィンドウにメンテナンスを行うようにスケジュールを変更するか、新しいウィンドウが構成されていない場合は自動的に新しいウィンドウを設定します。

トピック

メンテナンスが必要なフローの表示

メンテナンスが必要なフローは、MediaConnect コンソールまたは AWS CLI を使用して表示できます。

> **Note**
>
> フローに 必要期限日 (コンソール) または メンテナンス期限 (AWS CLI) がない場合は、そのフローのメンテナンスは現在必要ありません。

メンテナンスが必要なフロー (コンソール) を表示するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで、[Flows] (フロー) を選択します。
3. メンテナンスウィンドウ 列には、必要期限日 が表示されます。または、個々のフローの 詳細 ページで必要期限日 を確認することもできます。
4. 一覧表示されるすべてのフローは、表示された日付までに再起動する必要があります。

メンテナンスが必要なフロー (AWS CLI) を表示するには

- AWS CLI では、`list-flows` コマンドを使用してすべてのフローとそのメンテナンスステータスを表示できます。さらに、`describe-flow` コマンドを使用して特定のフローのメンテナンスステータスを表示できます。

```
aws mediaconnect list-flows
```

または

```
aws mediaconnect describe-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame
```

list-flows の戻り値の例を以下に示します。describe-flow の戻り値も同様の構造を使用します。

この例では、BasketballGameという名前のフローに、定期的なメンテナンスを行うための メンテナンス日 と メンテナンス開始時間 を設定しています。AwardsShowという名前のフローには、メンテナンス日 と メンテナンス開始時間 が設定されていますが、メンテナンス期限 も設定されています。メンテナンス期限 は、このフローでのメンテナンスの再起動に必要な期日です。また、AwardsShowフローでは MaintenanceScheduledDate の値からわかるように、メンテナンスの再起動を行う特定の日付もスケジュールしています。メンテナンスの予定日 は、メンテナンス期限 より前でなければなりません。

```
{
    "Flows": [
        {
            "AvailabilityZone": "us-west-2d",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
            "Name": "BasketballGame",
            "SourceType": "OWNED",
            "Status": "STANDBY",
            "Maintenance": {
                "MaintenanceDay": "Monday",
                "MaintenanceStartHour": "08:00"}
        },
        {
            "AvailabilityZone": "us-west-2b",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow",
            "Name": "AwardsShow",
            "SourceType": "OWNED",
            "Status": "ACTIVE",
            "Maintenance": {
                "MaintenanceDay": "Saturday",
```

```
                "MaintenanceDeadline": "2021-10-25T22:15:56Z",
                "MaintenanceScheduledDate": "2021-10-23",
                "MaintenanceStartHour": "23:00"}
        }
    ]
}
```

メンテナンスウィンドウの設定

メンテナンスイベントが発生する日と時刻を選択できます。これは メンテナンスウィンドウと呼ばれます。これらのウィンドウは、メンテナンスが本番稼働に与える影響を最小限に抑えるのに役立ちます。

メンテナンスウィンドウは、メンテナンスイベントが必要になるたびに使用されます。フローの作成時にメンテナンスウィンドウを設定したり、既存のフローにメンテナンスウィンドウを追加したりできます。メンテナンスウィンドウの曜日と時刻を変更するには、MediaConnect コンソールまたは AWS CLI を使用します。また、メンテナンスが必要な場合は、メンテナンスを実施する特定の日付を設定できます。選択する日付は、必要なメンテナンス日より前である必要があります。

メンテナンスウィンドウを設定しない場合、MediaConnect はフローを自動的に再起動します。メンテナンスが必要なフローごとにメンテナンスウィンドウを設定することをお勧めします。

メンテナンスウィンドウ (コンソール) を作成するには

1. MediaConnect コンソール (https://console.aws.amazon.com/mediaconnect/) を開きます。
2. ナビゲーションペインで、[Flows] (フロー) を選択します。フローにメンテナンスが必要な場合、メンテナンスウィンドウ 列に 必要期限 日が表示されます。
3. 1 つまたは複数のフローを選択します。フローごとに固有のメンテナンスウィンドウを設定できます。あるいは、複数のフローを選択してメンテナンスウィンドウを一括で設定することもできます。
4. フローのアクション ドロップダウンメニューで チャンネルメンテナンスウィンドウの編集 を選択します。
5.
   - 開始日 フィールドで、メンテナンスを行う曜日を選択します。
   - 開始時間 フィールドでメンテナンスを行う時間を選択します。時刻は UTC で指定します。
   - メンテナンスが必要な場合は、メンテナンスウィンドウ日 フィールドで特定の日付を選択できます。選択した日付は、必要なメンテナンス日時より前である必要があります。
   - [Update] (更新) を選択します。

6. 時間枠を確認するには、フロー ダッシュボードで メンテナンスウィンドウ 列を確認します。

メンテナンスウィンドウ (AWS CLI) を設定するには

1. AWS CLI で、update-flow コマンドを --maintenance オプションとともにを使用します。また、--flow-arn オプションを使用して作業するフローを指定する必要があります。

   --maintenance オプションは次の引数を取ります。

   - MaintenanceDay
   - MaintenanceStartHour
   - MaintenanceScheduleDate - この引数は、AWS によって必要なメンテナンス日が設定されている場合にのみ受け入れられます。

2. 次のコマンドを使用して、繰り返し発生するメンテナンスの日時を更新します。メンテナンスの日時は、必要なメンテナンスステータスに関係なく、いつでも設定できます。

```
aws mediaconnect update-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame --
maintenance MaintenanceDay='Tuesday',MaintenanceStartHour='10:00'
```

   次の例は、 メンテナンス日 と メンテナンス開始時間 のみを設定した場合の戻り値を示しています。

```
{
    "Flows": [
        {
            "AvailabilityZone": "us-west-2d",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:1-23aBC45dEF67hiJ8-12AbC34DE5fG:BasketballGame",
            "Name": "BasketballGame",
            "SourceType": "OWNED",
            "Status": "STANDBY",
            "Maintenance": {
                "MaintenanceDay": "Tuesday",
                "MaintenanceStartHour": "10:00"}
        }
    ]
}
```

3. 次のコマンドを使用して、繰り返されるメンテナンスの日時を設定するのに加えて、特定のメンテナンス日時を設定します。メンテナンス予定日は、AWS がフローのメンテナンスを必要とする場合にのみ設定できます。

```
aws mediaconnect update-flow --flow-arn arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow --maintenance
 MaintenanceDay='Saturday',MaintenanceStartHour='23:00',MaintenanceScheduledDate='2021-10-2
```

次の例は、メンテナンス日、メンテナンス開始時間、および メンテナンスの予定日 を設定したときの戻り値を示しています。

```
{
    "Flows": [
        {
            "AvailabilityZone": "us-west-2b",
            "Description": "Example flow description",
            "FlowArn": "arn:aws:mediaconnect:us-
east-1:111122223333:flow:2-3aBC45dEF67hiJ8k-2AbC34DE5fGa6:AwardsShow",
            "Name": "AwardsShow",
            "SourceType": "OWNED",
            "Status": "ACTIVE",
            "Maintenance": {
                "MaintenanceDay": "Saturday",
                "MaintenanceDeadline": "2021-10-25T22:15:56Z",
                "MaintenanceScheduledDate": "2021-10-23",
                "MaintenanceStartHour": "23:00"}
         }
    ]
}
```

選択した日時は、今後の定期的なメンテナンスイベントすべてに使用されます。この手順を繰り返して、メンテナンスウィンドウを追加または編集します。メンテナンスの完了後には、フロー ダッシュボードの メンテナンスステータス 列に 不要 が表示されます。

MediaConnect のベストプラクティス

最高のパフォーマンスと可用性を実現するには、ベストプラクティスに従って AWS Elemental MediaConnect フローを設定してください。

パフォーマンス

以下のベストプラクティスでは、トランスポートストリームフローのパフォーマンスを最適化する方法を説明します。

- トランスポートストリームフローの集計出力帯域幅が最大 400 MB/秒に設定されていることを確認してください。MediaConnect は、集計出力帯域幅が 400 MB/秒で動作するように設計されています。

  集計出力帯域幅 = (ソースのビットレート) x (出力数)

  たとえば、フローのソースのビットレートが 80 MB/秒で、出力が 5 の場合、集計出力帯域幅は 400 MB/秒です。同様に、ビットレートが 20 MB/秒のソースがあり、20 の出力にコンテンツを送信するフローの集計出力帯域幅も 400 MB/秒になります。

  > **Note**
  >
  > 1 つの ST 2110 JPEG XS 出力に対して 2 つの宛先を指定できるため、この計算ではこれらの出力を 2 回カウントする必要があります。

- メザニン品質のライブビデオでは、最大 120 メガビット/秒 (MB/秒) のビットレートでトランスポートストリームフローを設定できます。
- 富士通の出力は最大 20 個まで使用できます。20 個の富士通の出力に加え、富士通以外の出力は最大 30 個まで使用できます。集計出力帯域幅は 400 MB/秒を超えてはなりません。

以下のベストプラクティスでは、CDI フローのパフォーマンスを最適化する方法を説明します。

- CDI フローには最大 10 個の出力を使用できます。さらに、4Kp60 CDI フローは 10 個の ST 2110 JPEG XS 出力をサポートしますが、CDI 出力は 4 個のみです。

以下のベストプラクティスでは、ゲートウェイのパフォーマンスを最適化する方法を説明します：

- API を使用すると、複数のブリッジを一度に起動できます。API を使用して複数のブリッジを起動する場合は、一度に 10 個以下のブリッジを起動することをおすすめします。10 個を超えるブリッジを起動する必要がある場合は、複数のリクエストを使用してください。

可用性

- パケット損失を最小限に抑えるには、前方誤り訂正 (FEC) や Zixi や RTP-FEC プロトコルなどの自動リピートリクエスト (ARQ) ベースのプロトコルを使用してください。これらのプロトコルは、送信元デバイスと宛先デバイス間のパケット損失を最小限に抑えるように設計されています。
- AWS クラウドのような完全に管理されたネットワークであっても、どのネットワークでもパケット損失は発生するため、ワークフロー全体で冗長接続を作成して管理する必要があります。MediaConnect では、ワークフローに冗長性を加える方法が複数あります。
  - 少なくとも 2 つの異なるアベイラビリティーゾーンにフローを作成する。
  - 各フローに 2 つ目のソースを追加します。ストリームにエラーがある場合、MediaConnect は冗長ソースからのパケットを使用するか、冗長ソースに完全に切り替えることができます。
- 組織では、すべての AWS メディアサービス専用の VPC を作成することをお勧めします。単一の VPC は、IPアドレスの可用性を確保し、セキュリティグループに適切なルールを設定するのに役立ち、ネットワーク管理者が誤って伸縮性のあるネットワークインターフェイスを削除しないようにするのに役立ちます。

信頼性

- Amazon CloudWatch メトリックスとアラームを設定して、ソースの状態を追跡します。どのメトリクスをモニタリングするかについては、「モニタリングとタグ付け」を参照してください。

セキュリティ

- フローソースの CIDR ブロックはできるだけ正確でなければなりません。フローにコンテンツを提供する IP アドレスのみを含めてください。CIDR ブロックの幅が広すぎると、外部から第三者がフローにコンテンツを送信する可能性があります。
- SRT 出力を暗号化するために新しい SRT パスワードを作成する場合は、そのパスワードを AWS Secrets Manager で作成する必要があります。AWS Secrets Manager は特定のパスワードポリシーを強制しません。ただし、以下のパスワードポリシーを推奨します。

- パスワードの文字数制限: 10 ~ 80 文字
- 大文字、小文字、数字、**! @ # $ % ^ & * ( ) _ + - = [ ] { } | '** 記号のうち、最低 3 つの文字タイプの組み合わせ
- AWS アカウント名または E メールアドレスと同じでないこと

AWS Elemental MediaConnect におけるクォータ

以下の表では、制限と呼ばれていた AWS Elemental MediaConnect におけるクォータについて説明します。変更可能なクォータの詳細については、「AWS のサービスクォータ」を参照してください。

リソース	デフォルトのクォータ	コメント
使用権限管理	フローあたり 50	フローに付与できる使用権限の最大数。 このクォータを増やすことはできません。
フロー	AWS リージョンごとに 20	各 AWS リージョンで作成できるフローの最大数。 クォータの引き上げをリクエストできます。
[Outputs] (出力)	トランスポートストリームフローあたり 50 個 CDI フローあたり 10 個	フローが持つことができる出力の最大数。 このクォータを増やすことはできません。
[Sources] (出典)	トランスポートストリームフローあたり 2 つ CDI フローあたり 1 つ	フローが持つことができるソースの最大数。 このクォータを増やすことはできません。
VPC インターフェイス	フローあたり 2 つの ENA インターフェイスと 1 つの EFA インターフェイス	フローに保持できる VPC インターフェイスの最大数。 このクォータを増やすことはできません。

> **Note**
>
> パフォーマンスを最適化するには、集計出力帯域幅を 400 MB/秒以下に抑えるようにワークフローを設定することをお勧めします。詳細については、「ベストプラクティス」を参照してください。

API リクエストの制限

次の表に MediaConnect の API リクエスト頻度の制限を示します。これらの制限は、引き上げることができるクォータではありません。これらの制限を超えると、MediaConnect によって HTTP 429 (`too many requests`) エラーが返されます。

API メソッド	制限
API リクエストの頻度 - 定常状態	リージョン内の各アカウントに 1 秒あたり 5 リクエスト。 この制限は引き上げることができるクォータではありません。
API リクエストの頻度 - バーストモード バーストモードでは、定常状態の制限を一時的に超過する可能性があります。 API リクエストがバーストモードの制限を超えると、MediaConnect は制限をスロットルし、429 エラーを返します。 この制限は 1 秒あたり 5 リクエストのレートで補充されます。	リージョン内の各アカウントに 1 秒あたり 30 リクエスト。 この制限は引き上げることができるクォータではありません。

> **Note**
>
> アプリケーションがこれらの制限を超える場合は、再試行のエクスポネンシャルバックオフを実装することをお勧めします。詳細については、アマゾン ウェブ サービス全般のリファ

レンスの「AWS でのエラーの再試行とエクスポネンシャルバックオフ」を参照してください。

参考：対応メディア規格

> **Important**
>
> MediaConnect は、さまざまな組織の多くのメディア業界規格に準拠し、実装しています。このリファレンスは包括的なリストを意図したものではありませんが、特定の組織の主要な規格を掲載しています。

ビデオサービスフォーラム：技術的推奨事項

AWS Elemental MediaConnect は、一部の機能に対するビデオサービスフォーラム (VSF)からの技術推奨事項 (TR)をサポートしています。このリファレンスガイドは、MediaConnect がどの TR をサポートしているかを確認するために使用できます。技術的推奨事項の詳細については、VSF の Web サイト「VSF 技術的推奨事項」を参照してください。

サポートされている VSF 技術的推奨事項

技術的推奨事項	説明
TR-06-01： 信頼性の高いインターネットストリームトランスポート (RIST) [簡易プロファイル]	この技術的推奨事項は、RIST シンプルプロファイルサポートのみを対象としています。RIST を使用する場合、MediaConnect はメインプロファイル、拡張プロファイル、スケーラブルプロファイルをサポートしません。
TR-08： ST 2110-22 での JPEG XS ビデオのトランスポート **Note** ビデオフレームが MediaConnect によってエンコードされない JPEG XS パススルーフローの場合、ビデオフレームはデコードされません。そのため、TR-08 準拠の検証は行われません。	MediaConnect は SMPTE ST 2110-22 経由の JPEG XS トランスポートをサポートしていますが、以下の要件と制限があります。 • ハイプロファイルが必要です。メインプロファイルを使用しても エラーは発生しませんが、MediaConnect では無視されます。 • インターレース信号には、01 (トップフィールドファースト) のインターレースモードが必要です。

技術的推奨事項	説明
	• 3 ビット/ピクセルまたは 4 ビット/ピクセルのサブレベルが必要です。サブレベルは、使用する圧縮レベルとピクセルビット深度によって異なります。 • エンコードされたビデオフレームに配置されたビデオ説明ボックスには、プロファイル、インターレースモード、サブレベルのコンピラント値が反映されます。 • ネットワークメディアオープンスペシフィケーション (NMOS) 登録はサポートされていません。 • リアルタイムトランスポートプロトコル (RTP) シーケンシャルパケット送信モードのみ。 • コードストリームパケット化モードのみ。スライスモードはサポートされていません。 サポートされているカラースペース、ビット深度、およびクロマサンプリング構成： • YCbCr 10 ビット 4:2:2 • RGB 10 ビット 4:4:4 • RGB 12 ビット 4:4:4

SMPTE-2022

MediaConnect は、多くの SMPTE (米国映画テレビ技術者協会) 標準をサポートしています。以下の表は SMPTE-2022 に固有のもので、いくつかの標準が含まれています。これは、サポートされているすべての SMPTE 規格を包括的なリストにしたものではありません。

サポートされている SMPTE-2022 規格

規格	説明
SMPTE-2022-7： RTP のシームレスな保護スイッチング	• ソース：MediaConnect は、この規格に準拠する RTP ソースをサポートしています。ソースフェイルオーバーの詳細については、「ソースフェイルオーバー」を参照してください。 • 出力：RTP および RTP-FEC の出力は SMPTE 2022-7 規格に準拠しています。ダウンストリームにあるレシーバーが2022-7 のソースマージをサポートしている場合、RTP 出力と RTP-FEC 出力は互換性があります。

ユーザーガイドのドキュメント履歴

次の表は、AWS Elemental MediaConnect の今回のリリースのドキュメントをまとめたものです。このドキュメントの更新に関する通知については、RSS フィードでサブスクライブできます。

変更	説明	日付
API リクエストの制限	このガイドは、1 秒あたりの API リクエストの制限を含むように更新されました。	2023 年 11 月 2 日
AWS Elemental Link MediaConnect 搭載の UHD デバイス	AWS Elemental Link UHD デバイスと Zixi プッシュプロトコルを MediaConnect フローのソースとして使用できるようになりました。	2023 年 9 月 11 日
MediaConnect のメディアメトリクス	ユーザーガイドが更新され、MediaConnect を使用して送信されるメディアの状態を監視するための新しい CloudWatch メトリクスが追加されました。	2023 年 9 月 7 日
MediaConnect の高解像度メトリクス	MediaConnect のメトリクスを 1 秒という短い間隔で表示できるようになりました。	2023 年 6 月 22 日
サポートされているメディア標準リファレンス	このガイドは、MediaConnect がサポートするメディア業界規格の参照リストを含むように更新されました。	2023 年 6 月 9 日
SRT フェイルオーバー	ソースフェイルオーバーを有効にして、SRT (リスナーまたは発信者) ソースを含むフ	2023 年 5 月 1 日

	ローに 2 つ目のソースを追加できるようになりました。	
フェイルオーバーサポートテーブル	どのソースプロトコルがフェイルオーバーをサポートできるかを定義する新しいテーブルが追加されました。	2023 年 5 月 1 日
MediaConnect ゲートウェイメトリクス	ユーザーガイドが更新され、MediaConnect ゲートウェイ機能の新しい CloudWatch メトリクスが加わりました。	2023 年 4 月 13 日
AWS マネージドポリシー — 新しいポリシー	MediaConnectGatewayInstanceRolePolicy が作成されました。	2023 年 4 月 13 日
AWS マネージドポリシー — 新しいポリシー	AWS MediaConnectServicePolicy が作成されました。	2023 年 4 月 13 日
AWS Elemental MediaConnect Gateway	MediaConnect ゲートウェイと呼ばれる新機能がリリースされました。MediaConnect のオンプレミス実装における MediaConnect ゲートウェイ。	2023 年 4 月 13 日
AWSサービスにリンクされたロール - 新しいロール	AWSServiceRoleForMediaConnect ロールが作成されました。	2023 年 4 月 13 日
MediaConnect の IAM ガイダンスを更新しました	IAM のベストプラクティスに合わせてガイドを更新しました。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。	2023 年 2 月 14 日

Health CloudWatch イベント	フロー、ソース、および出力ヘルスモニタリングの新しいCloudWatchイベントがMediaConnect に追加されました。	2023 年 2 月 8 日
CDI プロトコルのカラーサポート	CDI プロトコルのカラースペース、ビット深度、クロマサンプリングサポートを定義する新しいテーブルが追加されました。	2022 年 11 月 4 日
MediaConnect アラート: ストリームエラー	ユーザーガイドが更新され、ストリームエラーアラートについての情報が含まれました。	2022 年 10 月 27 日
SRT コーラーのソースと出力	SRT コーラーのプロトコルをソースと出力に使用できるようになりました。	2022 年 9 月 19 日
ソースと出力プロトコルのテーブル	ソース、出力、またはその両方に使用できるプロトコルを定義する新しいテーブルが追加されました。	2022 年 8 月 5 日
メンテナンス CloudWatch メトリクス	ユーザーガイドが更新され、MediaConnect のメンテナンス用の新しい CloudWatch メトリクスが加わりました。	2022 年 8 月 1 日
メンテナンス CloudWatch イベント	ユーザーガイドが更新され、MediaConnect のメンテナンス用に新たに CloudWatch イベントが追加されました。	2022 年 8 月 1 日
SRT パスワード暗号化	SRT パスワード暗号化のドキュメントがガイドに追加されました。	2022 年 5 月 31 日

メンテナンスウィンドウ	MediaConnect のメンテナンスウィンドウをスケジュールして、フローのメンテナンスを実行できるようになりました。コンソールまたは API の新しいスケジューリングツールを使用して、メンテナンスをスケジュールできます。	2022 年 3 月 22 日
Fujitsu-QoS ソースと出力	ソースと出力に Fujitsu-QoS プロトコルを使用して、富士通デバイスとの間でコンテンツを送受信できるようになりました。	2021 年 12 月 20 日
メンテナンスウィンドウ	サポートケースを作成することで、MediaConnect のメンテナンスウィンドウをスケジュールしてフローのメンテナンスを実行できるようになりました。	2021 年 8 月 31 日
ソースフェイルオーバー	ソースフェイルオーバーを有効にするときに、2 つのソースのうちの 1 つをプライマリソースとして指定できます。ビデオストリームの中断を防ぐため、2 つのフェイルオーバーモードから選択できます。	2021 年 6 月 11 日
CDI ワークフロー	MediaConnect は、AWS クラウドデジタルインターフェイス (AWS CDI) の非圧縮ワークフロー用の JPEG XS をサポートするようになりました。	2021 年 5 月 17 日

リスナーのアドレス	リスナープロトコルを使用するフローでは、プライベートインターネットの出力送信 IP アドレスを簡単に見つけることができるようになりました。	2021 年 4 月 14 日
SRT リスナーのソースと出力	SRT リスナープロトコルをソースと出力に使用できるようになりました。	2021 年 3 月 16 日
予約	予約を購入できるようになりました。予約は、指定された期間中に毎月特定量のアウトバウンド帯域幅を使用するという約束と引き換えに、時間単位の料金を割引します。	2020 年 9 月 30 日
エンタイトルメントを無効にする	エンタイトルメントを無効化して、サブスクライバーのフローへのコンテンツのストリーミングを一時的に停止できるようになりました。アクセスを回復する準備ができたら、エンタイトルメントを有効にできます。	2020 年 7 月 24 日
ソースヘルスのメトリック	MediaConnect コンソールでは、一定期間のソースの状態を示す Amazon CloudWatch メトリクスを表示できます。	2020 年 5 月 11 日

VPC 出力	出力を追加して、パブリックインターネットを経由せずに AWS Elemental MediaConnect フローから VPC にコンテンツを送信できるようになりました。	2020 年 4 月 7 日
VPC ソース	パブリックインターネットを経由せずに VPC を AWS Elemental MediaConnect フローに接続し、フローにコンテンツを送信できるようになりました。	2020 年 3 月 31 日
ソースフェイルオーバー	ソースフェイルオーバーを有効にして、2 つ目の (冗長) ソースをフローに追加できるようになりました。	2020 年 3 月 13 日
Service Quotas (出力)	各トランスポートストリームフローに最大 50 個の出力を追加できます。	2020 年 2 月 7 日
エンタイトルメントデータの転送料金をサブスクライバーと共有します。	エンタイトルメントを付与するときに、サブスクライバーに負担させるエンタイトルメントデータ転送料金の割合を指定できるようになりました。	2019 年 9 月 16 日
RIST ソースと出力	RIST プロトコルをソースと出力に使用できるようになりました。	2019 年 9 月 11 日
Zixi プル出力	Zixi プルのプロトコルを使用する出力を追加できるようになりました。	2019 年 7 月 26 日

SPEKE サポート	(SPEKE) を使用してエンタイトルメントのコンテンツを暗号化できるようになりました。	2019 年 6 月 25 日
Service Quotas (フロー)	AWS リージョンあたり 20 フローのクォータへの増額をリクエストできます。	2019 年 3 月 14 日
新しいサービスとガイド	これは、メディアの取り込みおよび転送サービスである AWS Elemental MediaConnect と「AWS Elemental MediaConnect ユーザーガイド」の最初のリリースです。	2018 年 11 月 27 日

Note

- AWS Media Services は、生命の安全に関わるオペレーション、ナビゲーションや通信のシステム、航空管制、またはサービスの利用不能状態や中断または障害が、死亡事故や人身傷害、財産もしくは環境に対する損害につながる可能性のある (生命維持装置などの) アプリケーションとの併用や、フェイルセーフ性能を必要とする状況での使用を目的として設計または意図されていません。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。